United States General Accounting Office

GAO

Testimony

Before the Committee on Governmental Affairs
United States Senate

For Release on Delivery
Expected at
9:30 a.m.,
Tuesday
July 19, 1994

IRS AUTOMATION

Controlling Electronic Filing Fraud and Improper Access to Taxpayer Data

Statement of James F. Hinchman
Special Assistant to the Comptroller General
of the United States

GAO/T-AIMD/GGD-94-183

Mr. Chairman and Members of the Committee:

We are pleased to be here today to discuss the Internal Revenue Service's (IRS) efforts to (1) control the growing instances of fraud in the electronic filing program, (2) safeguard taxpayer automated files from unauthorized access and manipulation by IRS employees, and (3) remove unnecessary risk from its computer systems environment. These matters are critical to ensure that IRS issues proper refunds, has reasonable assurance that the confidentiality and accuracy of taxpayer data are protected, and has adequate computer systems security.

In recent years, the American public has come to expect quick access to information and services when dealing with private sector enterprises and now also expects the same responsiveness with federal government transactions. Today's automated technology has greatly increased IRS' ability to deliver services and to access information faster. Along with this technology has come new and greater challenges to protect IRS' highly sensitive taxpayer data.

IRS has recognized the problems associated with electronic filing fraud, browsing of taxpayer files by IRS employees, and a wider range of computer security weaknesses. IRS has taken some steps and plans to take others to improve these areas. However, additional action and sustained emphasis are necessary to improve controls over electronic filings and protect taxpayer information. This is especially important considering the upward trend in fraud associated with the electronic filing program, the unauthorized browsing by IRS employees of taxpayer files that IRS has identified as a problem in all of its regions, and the overall computer systems security risks IRS continues to face.

ELECTRONIC FILING FRAUD IS GROWING

Electronic filing shows the potential benefit of a paperless tax filing system. However, IRS has not yet shown how such a system can be adequately safeguarded against fraud. Electronic filing began as a demonstration project for Tax Systems Modernization and was offered nationwide in 1990. With this alternative to the traditional filing of paper returns, taxpayers could receive refunds within 2 weeks. Since 1990, the number of individual income tax returns filed electronically has increased--from 4.2 million then to 13.5 million this year. IRS views electronic filing as a cornerstone of its future business vision, and the goal is to receive 80 million electronically filed tax returns annually by 2001.

While we support the need to modernize IRS and the movement to electronic filing, we are concerned about the growing instances of electronic filing fraud. We recognize that electronic filing is not the only sources of filing fraud. Fraud associated with paper

filing is also a problem that has grown in recent years.[1] Further, electronic filing is not an avenue through which individuals can tap into IRS' tax data.

We agree with the electronic filing concept but stress the need for adequate systems security and controls to protect against fraudulent electronic returns. Thus far, the number of electronic returns identified as fraudulent in any 1 year has been relatively small--for example, in 1993, about 26,000 electronic returns were identified as fraudulent, worth over $50 million. However, the growth rate of such returns is high and it is unclear how much of the growth is due to an increase in fraudulent activity rather than an improvement in fraud detection. Even more troubling is the uncertainty as to how much fraud might be going undetected.

As of July 1, 1994, IRS had received 110.4 million individual income tax returns of which about 13.5 million were filed electronically--9.5 percent more than at the same time in 1993. By comparison, IRS reports show that 64 percent more fraudulent electronically filed returns were identified during the first 5 months of 1994 compared to the first 5 months of 1993--20,937 compared to 12,730.

If experience can predict future trends, many more fraudulent electronic returns will be identified by the end of the year. During the last 7 months of 1993, for example, IRS identified another 13,227 fraudulent electronic returns, bringing the annual total to just under 26,000. If the 64 percent growth rate during the first 5 months of 1994 remains constant during the rest of the year, the number of identified fraudulent electronic returns could increase to about 43,000 by the end of the year.

Electronic filing has made it easier for IRS to process returns because the tax information is submitted directly to IRS' computers. As a result, the paper return is eliminated and the time it takes to process a return is reduced. However, fraud detection is compromised because of the 2-week time constraint that IRS imposes on processing a return, the use of manual methods to identify fraudulent returns, and the lack of W-2 information to confirm wage earnings.

---

[1]In 1993, IRS reported identifying 51,883 fraudulent paper returns. The kind of fraud being perpetrated on electronically filed returns is no different than that being perpetrated on paper returns--for example, the preparation of bogus W-2s claiming fraudulent wages and withholdings; thus, supporting a fraudulent refund claim or earned income tax credit.

We have made several recommendations to improve IRS' controls over electronic filing fraud.[2] The recommendations, which I will now highlight, involved (1) improved screening and monitoring of persons and firms authorized to file returns electronically, (2) validations and editing in the electronic filing systems that would help prevent fraudulent electronic returns from being accepted, and (3) better detection of fraudulent returns that have been accepted.

Better Screening and Monitoring Preparers and Transmitters of Electronic Returns

One way to help prevent fraud is to ensure that only reputable preparers and transmitters file tax returns. To file electronically, taxpayers can either have an IRS-approved practitioner prepare and submit the return or take a return that has already been prepared to an individual or business that IRS has approved as a transmitter. Because some preparers and transmitters have been involved in schemes involving fraudulent electronic returns, we recommended in 1992 that IRS do more to check the backgrounds of persons applying to participate in the electronic filing program.

One step we recommended was that IRS obtain information from the Federal Bureau of Investigation (FBI) to identify preparer and transmitter applicants with prior criminal convictions. IRS is working with the FBI to obtain this information.

IRS can also rescind the electronic filing privilege of any electronic return preparer or transmitter who fails to abide by various operating requirements stipulated by IRS. The effect of this rescission authority, however, is mitigated by the absence of any servicewide procedure to prevent a barred preparer or transmitter from reapplying. To correct this problem, IRS is designing a system that can be used to screen preparers and transmitters.

Preventing Fraudulent Returns From Being Accepted

IRS does not adequately prevent fraudulent returns from being accepted. The aspect of electronic filing that most attracts taxpayers is the speed with which they can get refunds. That speed also makes electronic filing appealing to potential defrauders because IRS has less time to identify and stop questionable refunds once an electronic return has been accepted. One way to deal with the problem is to prevent questionable returns from being accepted.

---

[2]Tax Administration: IRS Can Improve Controls Over Electronic Filing Fraud (GAO/GGD-93-27, December 30, 1992) and Tax Administration: Increased Fraud and Poor Taxpayer Access to IRS Cloud 1993 Filing Season (GAO/GGD-94-65, December 22, 1993).

In this respect, electronic filing gives IRS an opportunity that it does not have with paper returns--the ability to verify the critical information on the return before accepting it and issuing a refund.

When IRS implemented the electronic filing system, it did not build in adequate validity checks to help protect against fraud. However, as the need for such checks became more apparent, IRS has implemented several. Now, before accepting an electronic return, for example, IRS verifies that the taxpayer's name and Social Security number on the electronic transmission match information in IRS' records. If there is a mismatch, IRS will not accept the return.

That validity check resulted in over 200,000 rejected returns in 1994. IRS does not know how many of the returns rejected through the various validity checks involved attempted fraud or how many were simply the result of errors by taxpayers or preparers in recording or transcribing names, Social Security numbers, or other data. Nonetheless, even with the various upfront controls and all of the rejections, the number of fraudulent electronic returns getting into the system and later being identified by IRS continues to increase.

Another potentially effective control would involve an automated comparison of wage data on tax returns with wage data provided by employers, which is not currently possible. Toward this end, IRS may have an opportunity to use partial-year data to at least verify that an employer/employee relationship exists and that the taxpayer's reported wages appear reasonable. To do this, IRS has been looking into the possibility of using quarterly wage data that employers submit to states for unemployment compensation purposes. In 1995, IRS plans to pilot such an effort in conjunction with the State of California. If use of this information proves feasible, IRS might be able to match three quarters of employer wage data against information on a taxpayer's return.

Detecting Fraudulent Returns

After returns are accepted, IRS uses computer screening criteria to identify questionable returns. These returns are then referred to analysts for various levels of review. This is a slow, labor intensive process that is not automated. The screening criteria are broad and generate many more questionable returns than can be reviewed by analysts, creating a backlog.

Despite the amount of effort devoted to this nonautomated review, relatively few fraudulent returns are actually identified. For example, of approximately 3 million potentially fraudulent returns IRS reviewed in 1993, almost 26,000 or less than 1 percent, were determined to be fraudulent.

IRS is taking steps to improve its screening/review process--steps that may produce more exacting criteria that better identify potentially fraudulent returns and help analysts do better in reviewing those returns. The major effort in this regard is a 4-year, four-phase initiative involving IRS and the Los Alamos National Laboratory. In the first phase, which was piloted in the IRS Cincinnati Service Center in 1994 and is to be implemented nationwide in 1995, IRS automated existing processes to, among other things, provide for on-line review of questionable returns and provide an interface to on-line databases to verify information on the return. The other three phases are expected to result in more sophisticated methods of detecting fraud and refining criteria for screening fraudulent returns for review.

THE RISK OF IMPROPER ACCESS TO TAXPAYER DATA CONTINUES

In August 1993, we testified before this Committee that IRS did not adequately control access authority given to computer support personnel or adequately monitor employee access to taxpayer information.[3] For example, in 1992, IRS' internal audit found that some employees had used their access (1) to monitor their own fraudulent returns, (2) to issue fraudulent refunds, and (3) to inappropriately browse through taxpayer accounts. We also reported on this matter as part of our audits of IRS' financial statements for fiscal years 1992 and 1993 under the Chief Financial Officers Act (Public Law 101-576).[4]

In its examinations of all of its regional offices, IRS found similar problems. IRS also reevaluated the disposition of the Southeast Region's suspected browsing cases. Of the 328 cases analyzed, the IRS Office of Ethics agreed with the disciplinary actions in 213 cases and disagreed in 83 cases. For the remaining 32 cases, the IRS Office of Ethics was unable to determine the appropriateness of the disciplinary action because of inadequate information.

Overall, the Office of Ethics concluded, and IRS management agreed, that the disciplinary actions in 51 of the 328 cases reviewed, or about 16 percent, were too lenient. Moreover, the Office of Ethics found cases of inconsistent punishment for similar offenses,

---

[3]Financial Management: First Financial Audits of IRS and Customs Revealed Serious Problems (GAO/T-AIMD-93-3, August 4, 1993).

[4]Financial Audit: Examination of IRS' Fiscal Year 1992 Financial Statements (GAO/AIMD-93-2, June 30, 1993), IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information (GAO/AIMD-93-34, September 22, 1993), and Financial Audit: Examination of IRS' Fiscal Year 1993 Financial Statements (GAO/AIMD-94-120, June 15, 1994).

including disparate treatment between offices and within the same office. In this regard, IRS revised penalty guidelines to set minimum and maximum penalties for violating computer security and privacy laws. The guidance provides important assistance to managers to encourage fair and consistent application of penalties.

An internal systems security study commissioned by IRS in 1993 pointed out that one of the greatest risks to security is from employees. Nevertheless, a December 1993 review by IRS' internal auditors found that there were virtually no controls programmed into the Integrated Data Retrieval System (IDRS) to limit what employees can do once they are authorized IDRS access and authorized to input account adjustments. The review indicated that IRS' internal security program had identified instances of employee attempts to embezzle funds using IDRS. IRS has planned corrective actions to limit the adjustments to an account, record details of each account transaction, and report unusual and high risk account adjustment activity.

IRS officials told us that some employees were confused and uncertain about whether IDRS security rules applied in certain circumstances and were unclear as to what actions constituted an improper access or unauthorized conduct. IRS has taken steps to better inform and educate employees on their responsibilities concerning IDRS security and privacy issues. These steps have included distributing articles and newsletters, showing videos, and forwarding a message from the Commissioner--all of which emphasize IRS' policy regarding proper use of tax data. We endorse these actions and in addition, believe that IRS needs to consistently apply appropriate penalties and publicize all disciplinary actions to heighten employees' awareness of security rules.

With the technology available today, unauthorized access to taxpayer accounts can be restricted with systems controls. IRS' August 1993 action plan to address security weaknesses in IDRS is attempting to move IRS in this direction. For example, IRS reports that it can now use system controls to detect and intervene if employees attempt to access their own accounts or those of their spouses. Similar restrictions are not yet implemented to control employee access to the accounts of others, such as neighbors, relatives, or celebrities.

IRS needs effective systems controls to not only restrict access to necessary taxpayer accounts but to record audit trails of virtually everything that goes on with taxpayers' accounts. Managers have the responsibility to monitor the use of the system to make sure it is secure. Since their time is limited, it is important that exception reports provide managers only the information needed to investigate potential problems. Such reports are planned as part of IRS' new Electronic Audit Research Log system.

IMPROVING IRS' OVERALL COMPUTER SYSTEMS SECURITY

Following the August 1993 hearing, we not only reviewed IRS' planned actions to correct IDRS' security problems but also made an assessment of the Service's overall computer systems security. IRS' overall computer controls do not adequately ensure that taxpayer data are adequately protected from unauthorized access, change, and disclosure or loss of operations due to disaster. Serious risks are not limited to the use of IDRS, but apply to other IRS systems which also provide access to taxpayer data. We found the following to be the primary weaknesses.

-- Inadequate control over access to computer systems. IRS' systems do not adequately prevent unauthorized access, which leaves taxpayer data at risk of illegal disclosure or alteration.

-- Limited monitoring of taxpayer account transactions. Access to tax accounts may not be recorded, or if recorded, provide insufficient information to investigate possible unauthorized access.

-- Poor contingency preparation for recovery after a disaster. This could leave IRS unable to provide basic tax processing services.

-- Improper management of software changes. This creates a risky systems environment where the systems could be sabotaged.

The details surrounding these problems and our recommendations for corrective action are being reported to the Committee separately and will be limited to official use only.

None of our overall computer systems security findings were new to IRS. In its 1993 Federal Managers' Financial Integrity Act report, IRS added security over taxpayer data as a material weakness. Over the last several years, IRS has commissioned a number of studies which have revealed these and other serious systems security problems. IRS is moving closer to resolving some of its long-standing computer security problems; but until the solutions are actually in place, serious risks remain.

Given the extent of the automated systems weaknesses, we advised IRS to conduct a comprehensive systems risk analysis that would identify the security vulnerabilities in its mission-critical operations and include the computer systems and the networks that connect them. We believe such an analysis is needed to ensure that all the major risks have been identified. Also, the analysis would enable IRS to determine whether the planned actions are sufficient to bring its computer security under adequate control.

IRS has demonstrated a strong commitment to improve control over access to its taxpayer records. Much of what IRS considers as its solution to its computer security problems is imbedded in the Tax Systems Modernization effort, which is 6 or more years away from completion.

Today's risks, however, cannot be left for a future system to resolve, and there are actions that can be taken today to secure IRS' computer systems. Implementing better automated systems controls through some of the technology options now available will require resources. Thus, IRS' managers face difficult but important decisions, such as deciding how many resources to devote to systems security in the current environment, given the commitment to Tax Systems Modernization.

- - - - -

Mr. Chairman, IRS is at a critical juncture--automating tax services is the essence of Tax Systems Modernization and IRS' ability to carry out its mission. This creates an entirely new set of challenges in managing IRS--controlling fraud and access to taxpayer data in an electronic age where technology is rapidly expanding. IRS is working to better control electronic filings and the great risk of unauthorized access to taxpayer account data and to improve overall computer systems security. IRS understands many of its underlying computer security weaknesses; but at the present time, serious and long-standing weaknesses remain. Adequately reducing the risk in these areas will depend on the prompt and effective implementation of significant computer systems security improvements. The continued oversight and support by this Committee in tackling this difficult challenge will also be most important.

This concludes my statement. We would be pleased to respond to any questions you or members of the Committee may have at this time.

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. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

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 (301) 258-4066.

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 (301) 258-4097 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

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

Bulk Mail
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested