United States General Accounting Office

GAO

Testimony

Before the Committee on Governmental Affairs
U.S. Senate

For Release on Delivery
Expected at
10 a.m.
Thursday,
April 10, 1997

IRS SYSTEMS SECURITY

Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses

Statement of Dr. Rona B. Stillman
Chief Scientist, Computers and Telecommunications
Accounting and Information Management Division

GAO/T-AIMD-97-76

Mr. Chairman and Members of the Committee:

We appreciate the opportunity to participate in this hearing on Internal Revenue Service (IRS) computer security weaknesses. Computer security problems are not unique to IRS. In fact, since June 1993, we have issued over 30 reports describing serious information security weaknesses at major federal agencies. Moreover, we reported in September 1996 that in the previous 2 years, serious information security control weaknesses had been reported for 10 of the 15 largest federal agencies.[1] This means that literally billions of dollars worth of assets are at risk of loss and vast amounts of sensitive data are at risk of unauthorized disclosure, modification, and destruction. Accordingly, we designated information security as a governmentwide high-risk issue in our 1997 report series on high-risk programs.[2]

Over the past several years, we have reported that IRS' management of computer security is ineffective and have made recommendations to strengthen computer security. Nevertheless, the GAO report that Senator Glenn has just released shows that IRS continues to have serious weaknesses in the controls used to safeguard IRS computer systems, facilities, and taxpayer data. These weaknesses could result in the disruption of tax processing operations or in the improper use, modification, or destruction of taxpayer data.

Computer security control weaknesses make IRS' computer resources and taxpayer data unnecessarily vulnerable to external threats, such as natural disasters and individuals or organizations with malicious intentions. They also increase IRS' vulnerability to internal threats, such as IRS employees accessing taxpayer files for purposes unrelated to their jobs (e.g., reading the files of celebrities or neighbors) or making unauthorized changes to taxpayer data, either inadvertently or deliberately for personal gain (e.g., to initiate unauthorized refunds or abatements of tax). These unauthorized and improper activities by IRS employees, which are commonly referred to as browsing, have been the focus of considerable attention in recent years, and have been of particular interest to this Committee. We found that despite this attention and interest, IRS is still not effectively addressing its browsing problem. IRS still does not effectively monitor employee activity, accurately record browsing violations, consistently punish offenders, or widely publicize reports of incidents detected and penalties imposed.

[1]Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, Sept. 24, 1996).

[2]High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

Before discussing each of these areas in greater detail, it is important to note that neither my statement nor our report that Senator Glenn just released quantifies the total number of weaknesses that we found or the number of weaknesses found in each of the eight functional categories of security that we reviewed. Additionally, neither my statement nor the report details the most serious weaknesses that we found. IRS officials were concerned that public disclosure of this information would increase the risks to their operations and employees. All of our findings have been reported in detail to the appropriate congressional committees.

Background

IRS relies on automated information systems to process over 200 million taxpayer returns and collect over $1 trillion in taxes annually. IRS operates 10 facilities throughout the United States to process tax returns and other information supplied by taxpayers. These data are then electronically transmitted to a central computing facility, where master files of taxpayer information are maintained and updated. A second computing facility processes and stores taxpayer data used by IRS in conducting certain compliance functions. There are also hundreds of other IRS facilities (e.g., regional and district offices) that use information systems to support tax administration.

IRS Computer Security Requirements

The Department of the Treasury requires IRS to have C2-level safeguards to protect the confidentiality of taxpayer data.[3] C2-level safeguards ensure "need-to-know" protection and controlled access to data. Similarly, IRS' Tax Information Security Guidelines require that all computer and communication systems that process, store, or transmit taxpayer data adequately protect these data, and the Internal Revenue Code prohibits the unauthorized disclosure of federal returns and return information.

Prior GAO Work on IRS Computer Security

Over the past 3 years, we testified and reported numerous times on serious weaknesses in security and other internal controls used to safeguard IRS computer systems and facilities. For instance, in August 1993, we identified weaknesses in IRS systems that hampered the Service's ability to effectively protect and control taxpayer data.[4] Subsequently, in

[3]The Department of Defense defines a hierarchy of security levels (i.e., A1, B3, B2, B1, C2, C1, and D), with A1 currently being the highest level of protection and D being the minimum level of protection.

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

December 1993, IRS identified taxpayer data security as a material weakness in its Federal Managers' Financial Integrity Act report.

In 1994, we reported, and IRS acknowledged, that while IRS had made some progress in correcting computer security weaknesses, IRS still faced serious and long-standing control weaknesses over automated taxpayer data. Moreover, we reported that these long-standing weaknesses were symptomatic of broader computer security management issues.

With respect to employee browsing, we reported in September 1993 that IRS did not adequately (1) restrict access by computer support staff to computer programs and data files or (2) monitor the use of these resources by computer support staff and users.[5] As a result, personnel who did not need access to taxpayer data could read and possibly use this information for fraudulent purposes. Also, unauthorized changes could be made to taxpayer data, either inadvertently or deliberately for personal gain (for example, to initiate unauthorized refunds or abatements of tax). In August 1995, we reported that the Service still lacked sufficient safeguards to prevent or detect unauthorized browsing of taxpayer information.[6]

Serious Computer Security Weaknesses Persist

Our on-site reviews of security at five facilities disclosed many weaknesses in eight functional areas. These areas are (1) physical security, (2) logical security,[7] (3) data communications management, (4) risk analysis, (5) quality assurance, (6) internal audit and security,[8] (7) security awareness, and (8) contingency planning. Of these eight, the primary weaknesses were in the areas of physical and logical security. Examples of weaknesses are discussed below.

Physical Security

Physical security and access control measures, such as locks, guards, fences, and surveillance equipment, are critical to safeguarding taxpayer data and computer operations from internal and external threats. We found many serious weaknesses in physical security at the facilities

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

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

[7]Logical security measures are safeguards incorporated in computer hardware and software.

[8]The phrases "internal audit" and "internal security" refer to functional disciplines, not IRS organizational entities.

visited. IRS has approved for public release only the following examples of physical security weaknesses:

- Collectively, the five facilities could not account for approximately 6,400 units of magnetic storage media, such as tapes and cartridges, which could contain taxpayer data. The number per facility ranged from a low of 41 to a high of 5,946.
- Fire suppression trash cans were not used in several facilities.
- Printouts containing taxpayer data were left unprotected and unattended in open areas of two facilities where they could be compromised.

Logical Security

Logical security controls limit access to computing resources to those personnel and programs with a need to know. Logical security control measures include the use of safeguards incorporated in computer hardware, system and application software, communication hardware and software, and related devices. We found numerous weaknesses in logical security at the facilities visited. Again, IRS has approved public disclosure of only the following examples:

- Tapes containing taxpayer data were not overwritten prior to reuse, providing the potential for unauthorized disclosure.
- Access to system software was not limited to individuals with a need to know. For example, at two facilities, we found that data base administrators[9] had access to system software, although their job functions and responsibilities did not require it.
- Application programmers were allowed to move development software into the production environment without adequate controls. In addition, these programmers were allowed to use taxpayer data for testing purposes, which places these data at unnecessary risk of unauthorized disclosure and modification.

Examples of Weaknesses in Other Functional Areas

Weaknesses were also found in the remaining six functional areas. For example, none of the facilities visited had conducted a complete risk analysis to identify and determine the severity of all the security threats to which they were vulnerable. Without these analyses, systems' vulnerabilities may not be identified and appropriate controls may not be implemented to correct them.

[9]The data base administrator is responsible for overall control of the data base, including its content, storage structure, access strategy, security and integrity checks, and backup and recovery.

Also, we found that two of the facilities had not performed an audit of operations within the last 5 years. Such internal audit and security reviews are needed to ensure that safeguards are adequate and to alert management to potential security problems.

Additionally, three of the five facilities did not have an adequate security awareness program. For example, one site had no process in place to ensure that management was made aware of security violations and security-related issues. An effective security awareness program is the means through which management communicates to employees the importance of security policies, procedures, and responsibilities for protecting taxpayer data.

Last, none of the five facilities visited had comprehensive disaster recovery plans. Specifically, we found that disaster recovery procedures at two of the five facilities had not been tested, while plans for the remaining locations were incomplete—i.e., they failed to include instructions for restoring all mission-critical applications and reestablishing telecommunications. Further, none had completed business resumption plans, which should specify the disaster recovery goals and milestones required to meet the business needs of their customers.

Electronic Browsing Is Not Being Addressed Effectively

IRS employee browsing of taxpayer information is another security threat that requires effective counter measures. To address this threat, IRS developed the Electronic Audit Research Log (EARL), an automated tool to monitor and detect browsing on the Integrated Data Retrieval System (IDRS).[10] IRS has also taken legal and disciplinary actions against employees caught browsing. However, EARL has shortcomings that limit its ability to detect browsing. In addition, IRS does not have reliable, objective measures for determining whether or not the Service is making progress in reducing browsing. Further, IRS facilities inconsistently (1) review and refer incidents of employee browsing, (2) apply penalties for browsing violations, and (3) publicize the outcomes of browsing cases to deter other employees from browsing.

EARL's Ability to Detect Browsing Is Limited

EARL cannot detect all instances of browsing because it only monitors employees using IDRS. EARL does not monitor the activities of IRS employees using other systems, such as the Distributed Input System, the Integrated Collection System, and the Totally Integrated Examination System, which

[10]IDRS is the primary computer system IRS employees use to access and adjust taxpayer accounts.

are also used to create, access, or modify taxpayer data. In addition, information systems personnel responsible for systems development and testing can browse taxpayer information on magnetic tapes, cartridges, and other files using system utility programs, such as the Spool Display and Search Facility,[11] which also are not monitored by EARL.

Further, EARL has some weaknesses that limit its ability to identify browsing by IDRS users. For example, because EARL is not effective in distinguishing between browsing activity and legitimate work activity, it identifies so many potential browsing incidents that a subsequent manual review to find incidents of actual browsing is time-consuming and difficult. IRS is evaluating options for developing a newer version of EARL that may better distinguish between legitimate activity and browsing.

IRS Progress in Reducing and Disciplining Browsing Cases Is Unclear

IRS' management information systems do not provide sufficient information to describe known browsing incidents precisely or to evaluate their severity consistently. IRS personnel refer potential browsing cases to either the Labor Relations or Internal Security units, each of which records information on these potential cases in its own case tracking system. However, neither system captures sufficient information to report on the total number of unauthorized accesses. For example, neither system contains enough information on each case to determine how many taxpayer accounts were inappropriately accessed or how many times each account was accessed. Without such information, IRS cannot measure whether it is making progress from year to year in reducing browsing.

A recent report by the IRS EARL Executive Steering Committee[12] shows that the number of browsing cases closed has fluctuated from a low of 521 in fiscal year 1991 to a high of 869 in fiscal year 1995.[13] However, the report concluded that the Service does not consistently count the number of browsing cases and that "it is difficult to assess what the detection programs are producing . . . or our overall effectiveness in identifying IDRS browsing."

Further, the committee reported that "the percentages of cases resulting in discipline has remained constant from year to year in spite of the Commissioner's 'zero tolerance' policy." IRS browsing data for fiscal years

[11]This utility enables a programmer to view a system's output, which may contain investigative or taxpayer information.

[12]Electronic Audit Research Log (EARL) Executive Steering Committee Report, (Sept. 30, 1996).

[13]We did not verify the accuracy and reliability of these data.

1991 to 1995 show that the percentage of browsing cases resulting in IRS' three most severe categories of penalties (i.e., disciplinary action, separation, and resignation/retirement) has ranged between 23 and 34 percent, with an average of 29 percent.[14]

Browsing Incidents Are Reviewed, Referred, Disciplined, and Publicized Inconsistently

IRS processing facilities do not consistently review and refer potential browsing cases. The processing facilities responsible for monitoring browsing had different policies and procedures for identifying potential violations and referring them to the appropriate unit within IRS for investigation and action. For example, at one facility, the analysts who identify potential violations referred all of them to Internal Security, while staff at another facility sent some to Internal Security and the remainder to Labor Relations.

IRS has taken steps to improve the consistency of its review and referral process. In June 1996, it developed specific criteria for analysts to use when making referral decisions. A recent report by the EARL Executive Steering Committee stated that IRS had implemented these criteria nationwide. Because IRS was in the process of implementing these criteria during our work, we could not validate their implementation or effectiveness.

IRS facilities are not consistently disciplining employees caught browsing. After several IRS directors raised concerns that field offices were inconsistent in the types of discipline imposed in similar cases, IRS' Western Region analyzed fiscal year 1995 browsing cases for all its offices and found inconsistent treatment for similar types of offenses. For example, one employee who attempted to access his own account was given a written warning, while other employees in similar situations, from the same division, were not counseled at all.

The EARL Executive Steering Committee reported widespread inconsistencies in the penalties imposed in browsing cases. For example, the committee's report showed that for fiscal year 1995, the percentage of browsing cases resulting in employee counseling ranged from a low of 0 percent at one facility to 77 percent at another. Similarly, the report showed that the percentage of cases resulting in removal ranged from 0 percent at one facility to 7 percent at another. For punishments other

[14]The mix among these three categories has remained relatively constant each year with disciplinary action accounting for the vast majority of penalties.

than counseling or removal (e.g., suspension), the range was between 10 percent and 86 percent.

IRS facilities did not consistently publicize the penalties assessed in browsing cases to deter such behavior. For example, we found that one facility never reported disciplinary actions. However, another facility reported the disciplinary outcomes of browsing cases in its monthly newsletter. By inconsistently and incompletely reporting on penalties assessed for employee browsing, IRS is missing an opportunity to more effectively deter such activity.

In conclusion, IRS' approach to computer security has not been effective. Serious weaknesses persist in security controls intended to safeguard IRS computer systems, data, and facilities. These weaknesses expose tax processing operations to the risk of disruption and taxpayer data to the risk of unauthorized use, modification, and destruction. Further, although IRS has taken some action to detect and deter browsing, it is still not effectively addressing this area of continuing concern because (1) it does not know the full extent of browsing and (2) it is addressing cases of browsing inconsistently.

Because of this, our report contains a series of specific recommendations, which if implemented, should greatly strengthen IRS computer security and effectively address its security risks. In summary, the report recommends that the IRS Commissioner (1) prepare a plan by April 30, 1997, for correcting all the weaknesses we identified at the five facilities we visited and for identifying and correcting security weaknesses at the other IRS facilities, (2) provide this plan to selected congressional committees, including the Senate Committee on Governmental Affairs, (3) report IRS' progress against this plan in its fiscal year 1999 budget submissions, (4) until corrected, report the security control weaknesses that we identified as material weaknesses in Treasury's Federal Managers' Financial Integrity Act reports, (5) by June 1997, reevaluate IRS' approach to computer security and report the results to selected congressional committees, including the Senate Committee on Governmental Affairs, (6) ensure that IRS completely and consistently monitors, records, and reports the full extent of electronic browsing, and (7) report IRS' progress in eliminating browsing in IRS' annual budget submission.

IRS has concurred with these recommendations and stated that it will implement them. We plan to monitor its progress in doing so to ensure that

security weaknesses are corrected and security management is strengthened.

Mr. Chairman, this concludes my statement. Lynda Willis, Director, Tax Policy and Administration Issues, and I will be happy to respond to any questions you or Members of the Committee might 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. 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.

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, or TDD (301) 413-0006.

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 touchtone 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 an 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

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