United States General Accounting Office

GAO

Report to the Ranking Minority Member, Committee on Governmental Affairs, U.S. Senate

April 1997

IRS SYSTEMS SECURITY

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

GAO/AIMD-97-49

GAO

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

Accounting and Information
Management Division

B-276609

April 8, 1997

The Honorable John Glenn
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

Dear Senator Glenn:

This report completes our response to your request to assess and report on Internal Revenue Service (IRS) computer security. While security is an area of paramount importance in all computer-based operations, it is particularly critical to IRS in light of the agency's vital revenue collection mission and the sensitivity of the data it processes. Accordingly, we agreed with your office to determine whether IRS is effectively (1) managing computer security and (2) addressing employee browsing of electronic taxpayer data.

On January 30, 1997, we issued to you a report responding to your request. The report detailed numerous security weaknesses that we found at five IRS facilities. Because some of the weaknesses are sensitive and could jeopardize IRS' security if released to the public, the report was designated "Limited Official Use" and the identities of the facilities that we visited were not disclosed. Subsequently, your office requested that we issue an excerpted version of the report suitable for public release. This report, which does not quantify either the total number of weaknesses found or the number of weaknesses found in specific functional categories, and does not detail the most serious weaknesses, satisfies that request. IRS commented on a draft of this report, and its comments have been included in this report, as appropriate. Details of our objectives, scope, and methodology are in appendix I.

Results in Brief

Over the last 3 years, we have reported on a number of computer security problems at IRS and have made recommendations for strengthening IRS' computer security management effectiveness. Nevertheless, IRS continues to have serious weaknesses in the controls used to safeguard IRS computer systems, facilities, and taxpayer data. Our recent on-site reviews of security at five facilities disclosed many weaknesses in the areas of (1) physical security, (2) logical security,[1] (3) data communications management, (4) risk analysis, (5) quality assurance, (6) internal audit and

[1]Logical security measures include safeguards incorporated in computer hardware and software.

security,[2] (7) security awareness, and (8) contingency planning. For example, the five facilities could not account collectively for approximately 6,400 missing units of magnetic storage media, such as tapes and cartridges, which could contain taxpayer data. In addition, printouts containing taxpayer data were left unprotected and unattended in open areas of two facilities where they could be compromised. Also, none of the facilities visited had comprehensive disaster recovery plans, which threaten the facilities' ability to restore operations following emergencies or natural disasters.

One area of unauthorized access that has been the focus of considerable attention is electronic browsing of taxpayer data by IRS employees. Despite this attention, IRS is still not effectively addressing the problem via thorough employee monitoring, accurate recording of browsing violations, or consistent application and publication of enforcement actions. For example, IRS currently does not monitor all employees with access to automated systems and data for electronic browsing activities. In addition, when instances of browsing are identified, IRS does not consistently investigate them or publicize them to deter others from browsing, and does not consistently punish browsers.

Until these serious weaknesses are corrected, IRS runs the risk of its tax processing operations being disrupted and taxpayer data being improperly used, modified, or destroyed.

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 support tax processing. Because of IRS' heavy reliance on systems, effective security controls are critical to IRS' ability to maintain the confidentiality of taxpayer data, safeguard assets, and ensure the reliability of financial management information.

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

Computer Security Requirements

The Computer Security Act[3] requires, among other things, the establishment of standards and guidelines for ensuring the security and privacy of sensitive information in federal computer systems. 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 outside IRS. To adequately protect the data, IRS must ensure that (1) access to computer data, systems, and facilities is properly restricted and monitored, (2) changes to computer systems software are properly authorized and tested, (3) backup and recovery plans are prepared, tested, and maintained to ensure continuity of operations in the case of a disaster, and (4) data communications are adequately protected from unauthorized intrusion and interception.

Also, Treasury requires IRS to have C2-level safeguards to protect the confidentiality of taxpayer data. 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. C2-level safeguards include all the requirements from the D and C1 levels and are required by IRS for all sensitive but unclassified data. These safeguards ensure need-to-know protection and controlled access to data, including

- a security policy that requires access control;
- identification and authentication that provide mechanisms to continually maintain accountability;
- operational and life-cycle assurances that include validations of system integrity and computer systems tests of security mechanisms; and
- documentation such as a security features user's guide, test documentation, and design documentation.

Prior GAO Work on IRS Computer Security

Over the past 3 years, we testified and reported numerous times on serious weaknesses with security and other internal controls used to safeguard IRS computer systems and facilities. For instance, in August 1993, we identified weaknesses in IRS' systems which hampered the Service's ability to effectively protect and control taxpayer data.[4] In this regard, we found that (1) IRS did not adequately control access given to computer support

[3]Public Law 100-235, 101 Stat. 1724 (1988).

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

personnel over taxpayer data and (2) established controls did not provide reasonable assurance that only approved versions of computer programs were implemented. Subsequently, in December 1993, IRS identified taxpayer data security as a material weakness in its Federal Managers' Financial Integrity Act report.

In 1994, we also reported, and IRS acknowledged, that while IRS had made some progress in correcting computer security weaknesses, IRS still faced serious and longstanding control weaknesses over automated taxpayer data. Moreover, we reported that these longstanding weaknesses were symptomatic of broader computer security management issues, namely, IRS' failure to (1) clearly delineate responsibility and accountability for the effectiveness of computer security within the agency and (2) establish an ongoing process to assess the effectiveness of the design and implementation of computer controls.[5] To address these issues, we recommended that IRS greatly strengthen its computer security management, and IRS agreed to do so.

The unauthorized electronic access of taxpayer data by IRS employees—commonly referred to as browsing—has been a longstanding problem for the Service. In October 1992, IRS' Internal Audit reported that the Service had limited capability to (1) prevent employees from unauthorized access to taxpayers' accounts and (2) detect an unauthorized access once it occurred.[6] 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.[7] 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.[8]

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

[6]Review of Controls Over IDRS Security, (IRS Internal Audit Reference Number 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]Financial Audit: Examination of IRS' Fiscal Year 1994 Financial Statements (GAO/AIMD-95-141, Aug. 4, 1995).

IRS Organizations Responsible for Managing Computer Security

Several organizations within the IRS are responsible for the security of IRS computer resources and the facilities that house them. For example, the Office of the Chief Information Officer is responsible for formulating policies and issuing guidelines for logical security, data security, risk analysis, security awareness, security management, contingency planning, and telecommunications. The Real Estate division within the Office of the Chief for Management and Administration is responsible for formulating policies and issuing guidelines for physical security. The field offices (e.g., service centers, computing centers, regional offices, district offices) are responsible for implementing these policies and guidelines at their locations. Compliance with the policies and procedures is assessed by both the headquarters and field offices.

Serious System Security Weaknesses Persist

Weaknesses in IRS' computer systems security continue to place taxpayer data and IRS' automated information systems at risk to both internal and external threats, which could result in the loss of computer services, or in the unauthorized disclosure, modification, or destruction of taxpayer data. While IRS has made some progress in protecting taxpayer data, serious weaknesses persist.

During our five on-site reviews, we found numerous weaknesses in the following eight functional areas: physical security, logical security, data communications management, risk analysis, quality assurance, internal audit and security, security awareness, and contingency planning.[9] Primary weaknesses were in the areas of physical and logical security.

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 weaknesses in physical security at the facilities visited. The following are examples of these 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.

[9]The order of the functional areas does not denote relative importance. Every area is crucial to protecting the security of IRS data and 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 only 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. Examples of these vulnerabilities include the following:

- Tapes containing taxpayer data were not overwritten prior to reuse.
- 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[10] 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.

Data Communications Management

Data communications management is the function of monitoring and controlling communications networks to ensure that they operate as intended and transmit timely, accurate, and reliable data securely. Without adequate data communications security, the data being transmitted can be destroyed, altered, or diverted, and the equipment itself can be damaged. At the five facilities, we found numerous communications management weaknesses.

Risk Analysis

The purpose of risk analysis is to identify security threats, determine their magnitude, and identify areas needing additional safeguards. We found risk analysis weaknesses at the five facilities. For example, none of the facilities visited 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 not implemented to correct them.

[10]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.

Quality Assurance

An effective quality assurance program requires reviewing software products and activities to ensure that they comply with the applicable processes, standards, and procedures and satisfy the control and security requirements of the organization. One aspect of a quality assurance program is validating that software changes are adequately tested and will not introduce vulnerabilities into the system. We found many weaknesses in quality assurance at the five facilities visited, including instances of failing to independently test all software prior to placing it into operation. In addition, when software products were tested, this testing was sometimes incomplete (e.g., did not include integrity or stress testing).[11] Such quality assurance weaknesses can result in systems not functioning properly, putting federal taxpayer data at risk.

Internal Audit and Security

Internal audit and internal security functions are needed to ensure that safeguards are adequate and to alert management to potential security problems. We found many weaknesses in the internal audit or internal security functions at the five facilities visited. For example, two of the facilities had not audited operations within the last 5 years.

Security Awareness

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. Three of the five IRS facilities did not have an adequate security awareness program. For example, at one site there was no process in place for ensuring that management was made aware of security violations and security related issues. We found several security awareness weaknesses at four of the five facilities.

Contingency Planning

A contingency plan specifies emergency response, backup operations, and post disaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. It addresses how an organization plans to deal with the full range of contingencies from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. It also identifies essential business functions and prioritizes resources in order of criticality. To be effective when needed, a contingency plan must be periodically tested and personnel trained in and familiar with its use.

[11]Integrity testing ensures that an application program performs only its intended functions. Stress testing assesses system performance at very high workloads.

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. We found many weaknesses in this functional area at the five sites visited.

Electronic Browsing Is Not Being Addressed Effectively

Taxpayer information can be compromised when IRS employees, who do not have a need to know, electronically peruse files and records. This practice, which is commonly called browsing, is an area of continuing serious concern. To address this concern, IRS developed an information system—the Electronic Audit Research Log (EARL)—to monitor and detect browsing on the Integrated Data Retrieval System (IDRS), the primary computer system IRS employees use to access and adjust taxpayer accounts. 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 know whether 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 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,[12] 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

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

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.

Because IRS does not monitor the activities of all employees authorized to access taxpayer data and does not monitor the activities of information systems personnel authorized to access taxpayer data for testing purposes, IRS has no assurance that these employees are not browsing taxpayer data and no analytical basis on which to estimate the extent of the browsing problem or any damage being done.

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. Consequently, for known incidents of browsing, IRS cannot efficiently determine how many and how often taxpayers' accounts were inappropriately 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[13] 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.[14] 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 "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 1991 to 1995 show that the percentage of browsing cases resulting in IRS'

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

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

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.[15]

Incidents of Browsing Are Reviewed and Referred Inconsistently

According to IRS, effectively addressing employee browsing requires consistent review and referral of potential browsing across IRS. However, 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 identified 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.

The analysts handle the review and referral of potential violations differently because IRS policies and procedures do not provide guidance in these areas. In June 1996, IRS' Internal Audit reported that IRS management had not developed procedures to ensure that potential browsing cases were consistently reviewed and referred to management officials throughout the agency.[16] Internal Audit further reported that analysts were not given clear guidance on where to refer certain cases, especially those involving potential Internal Security cases, and that procedures had been developed by some facilities but varied from site to site.

IRS has acted to improve the consistency of its 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.

Penalties for Browsing Are Inconsistent Across IRS

IRS policies and procedures on disciplining employees caught browsing direct IRS management to ensure that decisions are appropriate and consistent agencywide. After several IRS directors raised concern that field offices were not consistent in the types of discipline imposed in similar

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

[16]Implementation of the Electronic Audit Research Log (EARL), (IRS Internal Audit Ref. No. 064810, June 21, 1996).

cases, IRS' Western Region analyzed fiscal year 1995 browsing cases for all its offices and found inconsistent treatment for similar types of offenses. Examples of inconsistent discipline included

- Temporary employees who attempted to access their own accounts were given letters of reprimand, although historically, IRS terminated temporary employees for this type of infraction.
- 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 also 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 than counseling or removal (e.g., suspension), the range was between 10 percent and 86 percent.

Punishments Assessed for Browsing Not Consistently Publicized to Deter Violations

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. A representative at this facility told us that employees were generally aware of cases involving embezzlement and fraud if the cases received media attention. However, another facility reported the disciplinary outcomes of browsing cases in its monthly newsletter. For example, it cited a management official who accessed a relative's account and was punished. This facility publicized cases involving employees at all grade levels to emphasize that browsing taxpayer data is a serious offense punishable by adverse administrative actions or legal sanctions, including loss of job and criminal prosecution. By inconsistently and incompletely reporting on penalties assessed for employee browsing, IRS is missing an opportunity to more effectively deter such activity.

The EARL Executive Steering Committee noted that during the past 3 years IRS had published numerous documents intended to educate and sensitize employees to the importance of safeguarding taxpayer information. Nonetheless, the committee found that employees do not perceive the Service as aggressively pursuing browsing violations. It recommended that

communications be more focused and highlight actual examples of disciplinary actions that have been taken against employees who browse.

Conclusions

IRS' current approach to computer security is not effective. Serious weaknesses persist in security controls intended to safeguard IRS computer systems, data, and facilities and expose tax processing operations to the serious 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 inconsistently addressing cases of browsing.

Recommendations

Because of the serious and persistent security problems cited in our January 30, 1997, "Limited Official Use" version of this report, we recommended that the Commissioner of Internal Revenue, within 3 months of the date of that report, prepare a plan for (1) correcting all the weaknesses identified at the five facilities we visited, as detailed in the January 30, 1997 report, and (2) identifying and correcting security weaknesses at the other IRS facilities. We stated that this plan should be provided to the Chairmen and Ranking Minority Members of the Subcommittees on Treasury, Postal Service, and General Government, Senate and House Committees on Appropriations; Senate Committee on Finance; Senate Committee on Governmental Affairs; House Committee on Ways and Means; and House Committee on Government Reform and Oversight. We also stated that the Commissioner should report on IRS' progress on these plans in its fiscal year 1999 budget submission and should identify the computer security weaknesses discussed in this report as being material in its Fiscal Year 1996 Federal Managers' Financial Integrity Act report and subsequent reports until the weaknesses are corrected.

Also, because long-standing computer security problems continue to plague IRS operations, we reiterated our prior recommendation that the Commissioner, through the Deputy Commissioner, strengthen computer security management. In doing so, we recommended that the Commissioner direct the Deputy Commissioner to (1) reevaluate IRS' current approach to computer security along with plans for improvement, and (2) report the results of this reevaluation by June 1997, to above cited congressional committees and subcommittees.

Last, in light of the continuing seriousness of IRS employees' electronic browsing of taxpayer records, we recommended that the Commissioner ensure that IRS completely and consistently monitors, records, and reports the full extent of electronic browsing for all systems that can be used to access taxpayer data. We recommended that the Commissioner report the associated disciplinary actions taken and that these statistics along with an assessment of its progress in eliminating browsing, be included in IRS' annual budget submission.

Agency Comments and Our Evaluation

In commenting on a draft of this report, IRS agreed with our conclusions and recommendations and stated that it is working to correct security weaknesses and implement our recommendations. However, it did not commit to doing so for all recommendations within the time frames specified. Specifically, we recommended that by April 30, 1997, IRS develop a plan for (1) correcting all the weaknesses identified at the five facilities we visited and (2) identifying and correcting any security weaknesses at the other facilities. We specified this time frame because of the seriousness of the weaknesses we found. In our view, it is essential that IRS implement this recommendation expeditiously, and therefore we reiterate that IRS should complete the above cited plan by April 30, 1997.

Also concerning the correction of the weaknesses identified at the five facilities visited, IRS stated in its comments that "each facility is taking any corrective actions required by the GAO review." This statement is inconsistent with comments provided by each facility on its own weaknesses and thus evokes additional concerns about the need for a more concerted security management effort to ensure a consistent and effective level of security at all IRS facilities. Specifically, while the five facilities agreed with many of our findings and described appropriate corrective actions, they disagreed with many. In some cases, their comments reflected inconsistent views on the same problems. For example, some facilities acknowledged the need for fire suppression trash cans for disposing of combustible material (including paper) and chemicals in print rooms, while others disagreed. It is imperative that IRS recognize and correct security weaknesses systematically and consistently across all its facilities.

IRS also commented that "a recent reevaluation of the weaknesses by GAO's contractor identified that 41% of the weaknesses originally identified in the GAO report have already been corrected and closed, and an additional 12% were being adequately addressed by the facilities." Our contractor's

reevaluation assessment is not yet complete. Given the many serious security weaknesses yet to be fully dealt with or even addressed at this point, any preliminary assessment of IRS progress should be viewed with caution.

In addition, IRS stated that time did not permit it to report the weaknesses identified in our report as material in its fiscal year 1996 Federal Managers' Financial Integrity Act report. Instead, IRS has committed to reevaluating the status of material weaknesses that have and should be reported so that the fiscal year 1997 Federal Managers' Financial Integrity Act report will provide an accurate depiction of the agency's material weaknesses and coincide with its approach and plans for improvement.

The full text of IRS' comments on a draft of this report is in appendix II.

As agreed with your office, unless you publicly announce the contents of this report earlier, we will not distribute it until 30 days from the date of this letter. At that time, we will send copies to the Chairman, Senate Committee on Governmental Affairs, and the Chairmen and Ranking Minority Members of the (1) Subcommittees on Treasury, Postal Service, and General Government of the Senate and House Committees on Appropriations, (2) Senate Committee on Finance, (3) House Committee on Ways and Means, and (4) House Committee on Government Reform and Oversight. We will also send copies to the Secretary of the Treasury, Commissioner of Internal Revenue, and Director of the Office of Management and Budget. Copies will be available to others upon request.

If you have questions about this report, please contact me at (202) 512-6412. Major contributors are listed in appendix III.

Sincerely yours,

Dr. Rona B. Stillman
Chief Scientist for Computers
and Telecommunications

Contents

Abbreviations

EARL	Electronic Audit Research Log
GAO	General Accounting Office
IDRS	Integrated Data Retrieval System
IRS	Internal Revenue Service

Objectives, Scope, and Methodology

The objectives of our review were to (1) determine whether IRS is effectively managing computer security and (2) determine whether IRS is effectively addressing employee browsing of electronic taxpayer data.

To determine the effectiveness of IRS computer security, we first reviewed the findings from the computer security evaluation conducted by the public accounting firm of Ernst & Young in support of our audit of IRS' fiscal year 1995 financial statements. Ernst & Young's evaluation addressed general controls over such areas as physical security, logical security, communications, risk management, quality assurance, internal security, and contingency planning. Ernst & Young performed its evaluation at five IRS facilities, as well as IRS headquarters offices where it examined security policies and procedures.

Using Ernst & Young's evaluation results as preliminary indicators, we then evaluated and tested general computer security controls at the same five facilities in more depth. The areas we reviewed included physical security, logical security, data communications management, risk analysis, quality assurance, internal security and internal audit, security awareness, and contingency planning. Our evaluations included the review of related IRS polices and procedures; on-site tests and observations of controls in operation over all the systems in use at these locations; discussions of security controls with Integrated Data Retrieval System users, security representatives, and officials at the locations visited. Our evaluation did not include computer systems penetration testing.

We sent a letter reporting our findings to each IRS facility we visited, requesting comments and the outline of a plan for corrective actions. We then analyzed the responses and discussed the results with responsible IRS headquarters officials. We did not verify IRS' statements that certain actions had already been completed, but will do so as part of our audit of IRS' financial statements for fiscal year 1996.

To determine the effectiveness of IRS efforts to reduce employee browsing of taxpayer data, we reviewed documentation and discussed issues relating to the development and operation of the Electronic Audit Retrieval Log, the system IRS implemented to identify potential cases of employee browsing. We also reviewed data from the two systems IRS uses to track identified cases of browsing in order to determine the ability of these systems to accurately report the nature and extent of employee browsing. In addition, we discussed with IRS Internal Security officials the actions they are taking to investigate instances of browsing, and we

reviewed the Electronic Audit Research Log (EARL) Executive Steering Committee Report dated September 30, 1996.

To evaluate IRS' computer management and security, we assessed information pertaining to computer controls in place at headquarters and field locations and held discussions with headquarters officials. We did not assess the controls that IRS plans to incorporate into its long-term Tax Systems Modernization program.

We requested comments on a draft of this report from IRS and have reflected them in the report as appropriate. Our work was performed at IRS headquarters in Washington, D.C., and at five facilities located throughout the United States from May 1996 through November 1996. We performed our work in accordance with generally accepted government auditing standards.

Comments From the Internal Revenue Service

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

DEPUTY COMMISSIONER

March 27, 1997

Mr. Gene Dodaro
Assistant Comptroller General
United States General Accounting Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Dodaro:

We have received the draft report, IRS SYSTEMS SECURITY: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses, and would like to comment on three areas: unauthorized access of a taxpayer's account by an IRS employee ("browsing"); responsibility for security issues; and physical security.

Before doing so, I want to reaffirm that the Internal Revenue Service has long understood that safeguarding taxpayer information is essential to the operation of this country's self-assessment income tax system. That is why for many years the IRS has had in place policies and practices to protect the security and confidentiality of taxpayer information.

THE IRS DOES NOT TOLERATE BROWSING

Since concerns about browsing were first brought to the Commissioner's attention in 1993 by the IRS Chief Inspector, we have consistently stressed both inside and outside the Service that **unauthorized access of taxpayer accounts by IRS employees will not be tolerated**. In addition to communications to all employees, the Commissioner has also consistently emphasized in virtually every meeting, teleconference or other opportunity she has had to meet with employees that the IRS will not tolerate browsing. Warning messages have also been added to the "sign-on" screens for employees with access to taxpayer information databases. Your draft does not reflect these and the other steps taken by the Service in recent years to prevent browsing. Among the steps are:

- Expanding the ability to detect unauthorized accesses through the Electronic Audit Research Log (EARL);
- A Taxpayer Privacy and Security statement issued to all employees (October 20, 1993 -- copy enclosed);

Mr. Gene Dodaro

- A guide for disciplinary action emphasizing the seriousness of security violations and providing consistent discipline;
- Including information in various communications and training materials;
- A joint communication with NTEU to underscore the privacy policy and disciplinary liability for breach of the policy (November 16, 1994 -- copy enclosed);
- A memorandum to all employees reiterating the IRS Information Security Policy (January 3, 1995 -- copy enclosed);
- Enhancing the personnel information system, ALERTS, to track disciplinary outcomes so that consistency of disciplines can be monitored and evaluated; and
- Development and support for legislative changes that affirm criminal penalties for violations.

Enhancement of the EARL system, which detects potential unauthorized accesses by analyzing the audit trails of the almost 1.5 billion IDRS transactions each year, is currently the key to detection. Because of the volume of transactions and the extremely small percentage of potential unauthorized accesses, the Service is continuing to refine the EARL software to more efficiently identify such accesses.

Although effective detection, clear policies, communication, and training are important ways of institutionalizing a "zero tolerance" policy, strong disciplinary and judicial support are essential to reinforce the seriousness and consequences of violating the policy. In pursuing strong disciplinary actions before the Merit Systems Protection Board and the courts, the results thus far have been mixed. The Service has had particularly uneven success in sustaining strong discipline in the cases in which an employee has improperly accessed information, but not used the information for anyone's financial or other gain or detriment. These so-called "self disclosures," while violating IRS policy, have not always been viewed as seriously by third parties. Based upon this experience, the Service has supported legislative changes to Title 18 and Title 26 of the U.S. Code which would make browsing a criminal offense and permit dismissal of a guilty employee more readily. The recently passed Economic Espionage Act of 1996 (PL. 104-294) provides criminal misdemeanor penalties for anyone who intentionally accesses a computer without authorization or who exceeds authorized access and thereby obtains information from any department or agency of the United States. The IRS initiated action to include this provision in the Act. In addition, the Service is currently preparing guidance to management to limit the discretion of individual managers to determine the appropriate penalty for browsing.

In reference to GAO's concern that the IRS does not monitor the full extent of electronic browsing beyond IDRS, the IRS is reexamining systemwide security in the context of developing the overall modernized architecture. That approach would enable the Service to better control access to information through "up front"

authorizations and ultimately rely less on after-the-fact detection. In the interim, the feasibility of monitoring potential "browsing" on other systems that can be used to access taxpayer data is being assessed.

CENTRALIZED RESPONSIBILITY FOR SECURITY ISSUES HAS BEEN ESTABLISHED

Recognizing the critical need to enforce Federal law and regulations concerning privacy and non-disclosure of confidential tax information, the IRS has created an Office of Systems Standards and Evaluation (SSE) which assumes responsibility for establishing and enforcing standards and policies for all major security programs including, but not limited to, physical security, data security and systems security. Specifically, the SSE is responsible for :

- Approving standards and policies developed by operating units to ensure an integrated security plan;
- Assigning responsibilities across the IRS for systematically identifying, assessing, and mitigating risks;
- Promoting and ensuring user awareness of security issues;
- Evaluating the appropriateness and effectiveness of the actions taken to implement the standards and policies; and
- Providing feedback and recommendations to senior management to ensure compliance.

The SSE organization and approach are consistent with GAO's September 1996, report, Information Security: Opportunities for Improved OMB Oversight of Agency Practices, which noted that, "*Such a program can provide senior officials a means of managing information security risks and the related costs rather than just reacting to individual incidents.*" SSE is not intended to duplicate systems review efforts by the Office of the Chief Inspector which has focused on strengthening systems security, but rather is intended to add an enforcement capability within the Chief Information Officer organization, which spans the breadth of the IRS.

On January 6, 1997, Mr. Len Baptiste was appointed as the National Director of SSE. His past GAO systems evaluation management experience, including security issues, will provide the leadership needed to carry out the duties of this new Office.

Mr. Gene Dodaro

INCREASED INVESTMENTS WILL BE MADE IN PHYSICAL SECURITY

In the past because of financial and operational considerations, the IRS has reduced its investments in important systemic and physical security initiatives. The IRS support budgets have been decreased by over 14 percent, excluding training, in the past four years. While the Service believes that the difficult investment choices made between operational and security priorities have been wise, we also recognize that opportunities to improve security through risk assessments exist.

In the wake of the Oklahoma City bombing, Congress recognized the domestic terrorist threat to government facilities and appropriated $10.4 million in the FY '97 Counter Terrorism and Security Budget Amendment to provide additional protection for IRS facilities. To ensure the best investment of this appropriation, we are currently performing risk assessment and designing systems enhancements. Also, each facility is taking any corrective actions required by the GAO review. For example, a recent reevaluation of the weaknesses by GAO's contractor identified that 41% of the weaknesses originally identified in the GAO report have already been corrected and closed, and an additional 12% were being adequately addressed by the facilities. The Service is also developing a formal process to evaluate both information and physical security. This should assure that security standards are adhered to, corrective actions are taken, and that continual monitoring and evaluation of security occurs at all IRS facilities.

On March 3, 1997, Mr. William Hadesty was appointed as SSE's Director of Security Standards and Evaluations. Mr. Hadesty's private- and public-sector computer security experience includes over 10 years with the GAO, where he led comprehensive computer security reviews at numerous government agencies, including this review of IRS facilities. He is a recognized security expert in both the public and private sector. Mr. Hadesty is currently leading the Service's aggressive actions to correct security weaknesses and implement the following GAO recommendations to:

- Prepare a plan for correcting all the weaknesses identified at the five facilities reviewed by GAO and for identifying and correcting security weaknesses at the other IRS facilities;
- Provide the plan to the Chairmen and Ranking Minority Members of the Subcommittees on Treasury, Postal Service, and General Government, Senate and House Committees on Appropriations; Senate Committee on Finance; Senate Committee on Governmental Affairs; House Committee on Ways and Means; and House Committee on Government Reform and Oversight;

Mr. Gene Dodaro

- Report on IRS' progress against these plans in the fiscal year 1999 budget submission;
- Reevaluate IRS' current approach to computer security along with plans for improvement;
- Report the results of the reevaluation of the IRS' current approach by June 1997, to the above cited congressional committees and subcommittees;
- Completely and consistently monitor, record, and report the full extent of electronic browsing for all systems that can be used to access taxpayer data; and
- Report the associated disciplinary actions taken and that these statistics, along with an assessment of the Service's progress in eliminating browsing, be included in IRS' annual budget submission.

GAO's other recommendation for IRS to report the weaknesses identified in the GAO report as being material in our fiscal year 1996 Federal Managers Financial Integrity Act (FMFIA) report and subsequent reports until they are corrected, could not be included for 1996, because the GAO report was issued almost 3 months after issuance of our 1996 FMFIA report. However, IRS' Senior Council for Management Controls has tasked the SSE to reevaluate the status of all material weaknesses that have and should be reported, so that the 1997 FMFIA report provides an accurate depiction of our material weaknesses and coincides with our approach and plans for improvement.

In summary, nothing is more critical to the operation of our tax system than protecting taxpayer information. The actions the Service has taken and is taking will significantly strengthen current security. We look forward to working with you in this effort.

Sincerely,

Michael P. Dolan

Enclosures

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

COMMISSIONER

OCT 20 1993

MEMORANDUM FOR ALL EMPLOYEES

FROM: Margaret Milner Richardson
Commissioner, Internal Revenue Service

SUBJECT: Taxpayer Privacy and Security

One of the most important issues facing the IRS today is the privacy and security of taxpayer account information. Many of the changes we are experiencing right now, as well as the ones we hope to make, depend on our ability to protect private tax information.

In our daily work, we must continue to perform our duties in a manner that recognizes and enhances individuals' rights of privacy and ensures that our activities are consistent with laws, regulations, and good administrative practice. The Privacy Advocate, recently established under the Chief Information Officer to oversee the privacy concerns of the IRS and American taxpayers, has developed a Privacy Policy Statement. I fully endorse the attached statement, which gives a clear message about the importance of protecting taxpayers and employees from unnecessary intrusion into their tax records.

Any access of taxpayer information with no legitimate business reason to do so is unauthorized and improper and will not be tolerated. I made a pledge to Congress and I make it to you: taxpayer privacy and the security of tax data will not be compromised. We will discipline those who abuse taxpayer trust up to and including removal or prosecution.

The fundamental basis of our tax system, voluntary compliance, is directly affected by the level of trust taxpayers have in our ability to protect their information. The vast majority of IRS employees are dedicated and trustworthy. We must depend on each other's integrity and commitment to this agency and to keeping our tax system the best in the world.

Attachment (over)

Taxpayer Privacy Rights

The IRS is fully committed to protecting the privacy rights of all taxpayers. Many of these rights are stated in law. However, the Service recognizes that compliance with legal requirements alone is not enough. The Service also recognizes its social responsibility which is implicit in the ethical relationship between the Service and the taxpayer. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a taxpayer's privacy rights is an expectation that the Service will keep personal and financial information confidential. Taxpayers also have the right to expect that the Service will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry our agency responsibilities.

The Service will safeguard the integrity and availability of taxpayers' personal and financial data and maintain fair information and recordkeeping practices to ensure equitable treatment of all taxpayers. IRS employees will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our recordkeeping practices, the Service will respect the individual's exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the Service takes very seriously its social responsibility to taxpayers to limit and control information usage as well as to protect public and official access. In light of this responsibility, the Service is equally concerned with the ethical treatment of taxpayers as well as their legal and administrative rights.

Approved: Margaret M. Richardson Date: 10/15/93
Commissioner

COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224
NOV 16 1994

MEMORANDUM FOR ALL EMPLOYEES

FROM: Margaret Milner Richardson
Commissioner of Internal Revenue

Robert M. Tobias
President, National Treasury Employees Union

SUBJECT: Privacy and Security of Taxpayer Information

Safeguarding public confidence in the integrity and competence of the Service is a top priority for all employees. Each of us must take seriously any perceived or real breach in public confidence and trust in our ability to administer tax laws. The availability of taxpayer information, or any other protected data, dictates a responsibility to observe privacy principles, to secure sensitive data, and to guard against improper disclosures. Clearly, most Service employees are conscientious and respect the taxpayer's right to expect that the information they provide will be safeguarded. However, any one breach by any one of us seriously undermines public confidence and trust in the Service.

Improper access to, or misuse of, taxpayer information violates law, rule, and regulation and is contrary to our ethical values and principles of public trust. In October 1993, the Service issued a Privacy Policy Statement. The policy emphasizes comprehensive privacy, security, and disclosure requirements. It also represents an application of Service ethical values and principles of public trust in our day-to-day operations. This year, we began to strengthen our commitment to the protection of taxpayer privacy through the Declaration of Privacy Principles and the issuance of the Guide for Penalty Determinations. Each of you received a copy of these documents and we urge you to become familiar with their contents.

MEMORANDUM FOR ALL EMPLOYEES

Our efforts to maintain taxpayer privacy also includes continually improving Service ability to identify any employee who fails to safeguard taxpayer information and, where appropriate, taking disciplinary action, up to and including removal. This effort is not intended to impose an additional burden on conscientious employees in their use of tax systems. It is, however, intended as a concerted effort to maintain a work environment that reflects the highest standard for the protection of sensitive taxpayer information.

Privacy, security and disclosure issues will continue to be a major consideration and top priority for you as our Compliance 2000 and Tax Systems Modernization efforts lead to the identification of innovative approaches to the protection of taxpayer privacy. Each of us must continually examine how we accomplish our duties and be ever vigilant in safeguarding taxpayer privacy.

COMMISSIONER

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

January 3, 1995

MEMORANDUM FOR ALL EMPLOYEES

FROM: Margaret Milner Richardson
Commissioner of Internal Revenue

SUBJECT: IRS Information Security Policy

Privacy, security and disclosure issues are key elements for the success of our Compliance 2000 and Tax Systems Modernization efforts. The success of the Service in addressing privacy, security and disclosure issues also has a critical impact on voluntary compliance, the fundamental basis of our tax system. Therefore, it is mandatory for each of us to secure sensitive data and guard against improper disclosures.

In October 1993, the Service issued a Privacy Policy Statement developed by the Privacy Advocate. A related document, the IRS Information Security Policy, has been developed by the System Architect's Office under the direction of the Chief Information Officer. The intent of this policy, which is attached, is threefold:

Ensure that the Service complies with the applicable guidance from public laws, regulations, and directives.

Ensure that taxpayer and other sensitive information is protected commensurate with the risk and magnitude of the harm that would result from inappropriate use.

Ensure that taxpayer and other sensitive information is used only for necessary and lawful purposes.

I fully endorse the attached policy statements.

I made a pledge to Congress and I make it to you: taxpayer privacy and the security of tax data will not be compromised. The implementation of the IRS Information Security policy is an important step in fulfilling this pledge.

Attachment

IRS Information Security Policy

P1. It is the policy of the IRS to establish and enforce a comprehensive and appropriate security program that assures IRS information resources are protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such resources.

P2. It is the policy of the IRS to collect, use, maintain, and disseminate only that information required for a necessary and lawful purpose.

P3. It is the policy of the IRS to ensure that its information collection, use, storage, dissemination, and derivation processes maintain the accuracy of the information relative to its intended use.

P4. It is the policy of the IRS to ensure that all information and resources required by an authorized individual to perform an assigned function are complete and available when required.

P5. It is the policy of the IRS to collect, use, maintain, and disseminate information with appropriate timeliness to ensure successful completion of IRS business functions.

P6. It is the policy of the IRS to limit access to IRS information and resources to authorized individuals who have a right to the information or resource or a demonstrable need for the information or resource to perform official duties.

P7. It is the policy of the IRS to disclose information to organizations or individuals outside of the IRS only when such disclosure is consistent with public law and other governing regulations.

P8. It is the policy of the IRS to ensure that only functions required for a necessary and lawful purpose be performed on IRS information or resources.

P9. It is the policy of the IRS to prevent, or to detect and counter, fraud.

P10. It is the policy of the IRS to ensure the continuity of operation of activities that support critical agency functions.

P11. It is the policy of the IRS to establish and enforce security procedures for persons involved in the design, development, operation, or maintenance activities that affect the protection of IRS information and resources.

P12. It is the policy of the IRS to ensure that its work force has the technical and awareness training, appropriate to level of responsibility and authority, to implement and adhere to an IRS security program.

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

Randolph C. Hite, Senior Assistant Director
Ronald W. Beers, Assistant Director
Ronald E. Parker, Senior Information Systems Analyst
Ronald E. Famous, Senior Information Systems Analyst
Gary N. Mountjoy, Assistant Director

Atlanta Field Office

Carl L. Higginbotham, Senior Information Systems Analyst
Glenda C. Wright, Senior Information Systems Analyst
Teresa F. Tucker, Information Systems Analyst

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

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