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

Accounting and Information
Management Division

B-277242

June 23, 1997

The Honorable Ben Nighthorse Campbell
Chairman, Subcommittee on Treasury and
General Government
The Honorable Herb Kohl
Ranking Minority Member, Subcommittee on
Treasury and General Government
Committee on Appropriations
United States Senate

Subject: IRS Systems Security and Funding: Additional Information on Employee Browsing and Tax Systems Modernization

In our April 15, 1997, testimony before your Subcommittee, we reported on the Internal Revenue Service (IRS) employees' electronic browsing of taxpayer files and IRS' fiscal years 1998 and 1999 budget requests for tax systems modernization.[1] Enclosed are our responses to additional questions received from you on April 22, 1997, for the hearing record. Enclosure I contains responses to Chairman Campbell's questions, and enclosure II contains responses to Senator Kohl's questions.

A copy of this letter is also being sent to the Acting Commissioner of IRS. Please contact me at (202) 512-6412 or Lynda Willis, Director, Tax Policy and Administration Issues, General Government Division, at (202) 512-9110, if you have questions regarding our responses.

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

Enclosures

[1]IRS Systems Security and Funding: Employee Browsing Not Being Addressed Effectively and Budget Requests for New Systems Development Not Justified (GAO/T-AIMD-97-82, April 15, 1997).

RESPONSES TO QUESTIONS ON IRS COMPUTER SECURITY AND ELECTRONIC BROWSING

QUESTIONS SUBMITTED BY CHAIRMAN CAMPBELL

GAO Discovery of Browsing

Question: Based on what you have found, how common do you believe the browsing problem is at IRS?

GAO Response: IRS does not collect sufficient information or sufficiently monitor employee access to taxpayer data to determine the full extent of its browsing problem. For example, information collected on each potential browsing case does not include the number of taxpayer accounts inappropriately accessed or how many times each account was accessed. A recent IRS study of browsing at 10 service centers also concluded that the Service did not consistently count the number of browsing cases, and that it was difficult to assess the overall effectiveness of IRS efforts to identify the extent of browsing.

Also, IRS electronically monitors only employees who use the Integrated Data Retrieval System (IDRS). IRS does not monitor the activities of IRS employees that use 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, which also are not monitored by IRS.

Current IRS Procedures and Standards

Question: How would you qualify the IRS' current standards?

GAO Response: IRS' approach to computer security, which includes definition, implementation, and enforcement of security policies and procedures (i.e., standards), is not effective. Accordingly, we recommended that IRS reevaluate its current approach to computer security, along with plans for improvement, and report the results to selected congressional committees and subcommittees.[1]

---

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

Question: Are there government or industry standards for the protection of this type of sensitive information? What are these standards based on?

GAO Response: Various federal laws and guidance govern the protection of sensitive and critical federal data. The Privacy Act of 1974; the Paperwork Reduction Act of 1980, as amended; and the Computer Security Act of 1987 all contain provisions requiring IRS and other agencies to protect the confidentiality and integrity of the sensitive information that they maintain. The Computer Security Act (Public Law 100-235) defines sensitive information as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under [the Privacy Act], but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

The adequacy of security and other internal controls over computerized data is also addressed indirectly by the Federal Managers' Financial Integrity Act (FMFIA) of 1982 (31 U.S.C. 3512(b) and (c)) and the Chief Financial Officers (CFO) Act of 1990 (Public Law 101-576). FMFIA requires agency managers to annually evaluate their internal control systems and report to the President and the Congress any material weaknesses that could lead to fraud, waste, and abuse in government operations. The CFO Act requires agency CFOs to develop and maintain financial management systems that provide complete, reliable, consistent, and timely information. Under the act, major federal agencies, such as IRS, annually issue audited financial statements. In practice, such audits generally include evaluating and testing controls over information security.

In accordance with the Paperwork Reduction Act of 1980 (Public Law 96-511), the Office of Management and Budget (OMB) is responsible for developing information security policies and overseeing agency practices. In this regard, OMB has provided guidance for agencies in OMB Circular A-130, appendix III, "Security of Federal Automated Information Resources." Since 1985, this circular has directed agencies to implement an adequate level of security for all automated information systems that ensures (1) effective and accurate operations and (2) continuity of operations for systems that support critical agency functions. The circular establishes a minimum set of controls to be included in federal agency information system security programs and requires agencies to review systems security at least every 3 years. Responsibility for developing technical standards and providing related guidance for sensitive data belongs primarily to the National Institute of Standards and Technology (NIST), under the Computer Security Act. OMB, NIST, and agency responsibilities for information security were recently reemphasized in the Clinger-Cohen Act.

Question: Can you provide this subcommittee an outline of current IRS standards and procedures relating to the security of taxpayers' files?

GAO Response: IRS security standards and procedures for taxpayer files are in the Internal Revenue Code, IRS' Tax Information Security Guidelines, IRS' Information Security Policy, and Department of the Treasury guidance. The Internal Revenue Code prohibits the unauthorized disclosure of federal returns and return information outside IRS. IRS' Tax Information Security Guidelines require that all computer and communication systems that process, store, or transmit taxpayer data adequately protect these data. The Service's information security policy mandates that taxpayer information is to be used only for necessary and lawful purposes.

In addition, the Department of the 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, C2, C1, and D) with A1 being the highest level of protection and D the lowest. Each level of safeguards includes all the requirements of lower levels. C2-level safeguards are required by IRS for all sensitive but unclassified data. These safeguards are designed to ensure need-to-know protection and controlled access to data, including a security plan that requires access control; identification and authentication that provide mechanisms to continually maintain accountability; operational and lifecycle 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.

Question: The Committee is concerned that the IRS is unable to closely monitor its employees' access to files. What do you believe is the best course of action for IRS in terms of technology and procedures that it can implement to better monitor its systems and employees?

GAO Response: As we recommended in our April 1997 report and testimony,[2] the IRS Commissioner needs to 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. In this regard, IRS needs to address the fact that the system it developed to monitor and detect browsing–the Electronic Audit Research Log (EARL)–does not have the capability to detect all instances of browsing. While EARL monitors

---

[2]IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, April 8, 1997) and IRS Systems Security and Funding: Employee Browsing Not Being Addressed Effectively and Budget Requests for New Systems Development Not Justified (GAO/T-AIMD-97-82, April 15, 1997).

those employees using the Integrated Data Retrieval System, it does not monitor the activities of IRS employees using other systems which are also used to create, access, or modify taxpayer data, such as the Distributed Input System, the Integrated Collection System, and the Totally Integrated Examination System. IRS is evaluating options for developing a newer version of EARL with the ability to distinguish between legitimate activity and browsing. We encourage IRS to move forward with this effort, but caution that until employee activity is effectively monitored on all systems used to access taxpayer data, IRS has no effective means to monitor employee browsing.

Question: In your estimation, is it currently possible for the IRS to monitor employees well enough to avoid a case of mistaken identity of an employee who is browsing?

GAO Response: While our work did not specifically focus on whether IRS has the capability to avoid this type of situation, we did review agency processes for investigating browsing incidents. These processes include discussing matters under investigation with involved employees. Having these discussions allows employees an opportunity to explain instances of mistaken identity and IRS to consider this as a possible explanation for accessing taxpayer information.

Question: Can GAO please provide the subcommittee with a recommendation as to which procedures should be put in place by IRS to discourage future incidents of browsing and how it can ensure the consistent implementation of punishments?

GAO Response: As we recommended in our April 1997 report and testimony,[3] the IRS Commissioner should 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 and reports the associated disciplinary actions taken against employees caught browsing. In doing this, IRS will need to enhance its capability to detect instances of browsing and ensure that its policies and procedures on disciplining employees caught browsing are applied consistently agencywide.

[3]GAO/AIMD-97-49, April 8, 1997, and GAO/T-AIMD-97-82, April 15, 1997.

QUESTIONS SUBMITTED BY SENATOR KOHL

Question: The GAO's office has been very thorough in its review of the IRS and of its Tax Systems Modernization efforts. Numerous reports have been issued and numerous recommendations have been made. I am concerned about the fundamental management problems within the IRS. Can you please tell us what progress you have seen the IRS make over the past five years as it relates to its management problems?

GAO Response: IRS is taking some steps to address fundamental management problems, but the Service has been slow in implementing our recommendations aimed at correcting these problems. As a result, many management problems remain.

For example, the one factor that has most contributed to IRS' problems is the absence of the kind of data (operational and financial) needed to effectively manage such a large organization. We have commented many times, for example, on the impact of incomplete information on IRS' efforts to efficiently and effectively collect delinquent taxes. Good data are also needed if IRS is to bring to fruition its efforts to develop and track the kind of performance measures (such as return on investment) that are needed to effectively manage the agency and make critical resource allocation decisions. IRS has made some strides in accumulating more useful data, but much more needs to be done. It is this need, more than anything, that makes systems modernization so critically important.

In another instance, we briefed IRS management in early 1995 and later issued a report[1] in July 1995 detailing pervasive management and technical weaknesses with IRS' Tax Systems Modernization (TSM) program. At that time, we made over a dozen recommendations to the IRS Commissioner to address these weaknesses.

Collectively, the recommendations called for IRS to (1) formulate a comprehensive business strategy for maximizing electronic filings, (2) improve IRS' strategic information management by implementing a process for selecting, prioritizing, controlling, and evaluating the progress and performance of all major information systems and investments, (3) implement disciplined, consistent procedures for software requirements management, quality assurance, configuration management, and project planning and tracking, and (4) complete and enforce an integrated systems architecture and security and data architectures. IRS concurred with our findings and conclusions and agreed to implement our recommendations.

---

[1]Tax Systems Modernization: Management and Technical Weaknesses Must Be Corrected If Modernization Is To Succeed (GAO/AIMD-95-156, July 26, 1995).

Pursuant to congressional direction, we assessed IRS' actions, as delineated in Treasury's report on tax systems modernization, to correct its management and technical weaknesses. Specifically, we reported in June and September 1996[2] that while IRS had initiated many activities to improve its modernization efforts, it had not yet fully implemented any of our recommendations. Consequently, in order to minimize the risk attached to continued investment in systems modernization, we suggested to the Congress that it consider limiting modernization funding to only cost-effective efforts that (1) support ongoing operations and maintenance, (2) correct IRS' pervasive management and technical weaknesses, (3) are small, represent low technical risk, and can be delivered quickly, and (4) involve deploying already developed and fully tested systems that have proven business value and are not premature given the lack of a completed architecture.

To help improve IRS' modernization and correct persisting management and technical weaknesses, the Congress in the fiscal year 1997 Omnibus Consolidated Appropriations Act, directed IRS to (1) submit by December 1, 1996, a schedule for transferring a majority of its modernization development and deployment to contractors by July 31, 1997, and (2) establish a schedule by February 1, 1997, for implementing GAO's recommendations by October 1, 1997. In its conference report on the act, the Congress directed the Secretary of the Treasury to (1) provide quarterly reports on the status of IRS' corrective actions and modernization spending[3] and (2) submit, by May 15, 1997, a technical architecture for the modernization that has been approved by Treasury's Modernization Management Board. Also, the Board was directed to prepare a request for proposals by July 31, 1997, to acquire a prime contractor to manage modernization deployment and implementation or face suspension of funding for TSM operational systems.

IRS has continued to take steps to address our recommendations and respond to congressional direction. For example, IRS hired from outside the agency, a new Chief Information Officer and a Director of the Service's newly created Government Program Management Office (GPMO). It also created an investment review board to select, control, and evaluate its information technology investments. Thus far, the board has

---

[2]Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses (GAO/AIMD-96-106, June 7, 1996) and Tax Systems Modernization: Actions Underway But Management and Technical Weaknesses Not Yet Corrected (GAO/T-AIMD-96-165, September 10, 1996).

[3]H.R. Report No. 863, 104th Cong., 2d Session (1996). The Congress also included the requirement that Treasury provide a milestone schedule for developing and implementing all modernization projects in Treasury's fiscal year 1996 appropriations act (Public Law 104-52, 109 Stat. 474, November 19, 1995).

reevaluated and terminated selected major TSM development projects, such as the Document Processing System. In addition, IRS provided a November 26, 1996, report to the Congress that set forth IRS' strategic plan and schedule for shifting modernization development and deployment to contractors.

IRS has other actions underway to strengthen TSM management. For example, it is developing a comprehensive strategy to maximize electronic filing. It is also updating its system development life cycle methodology and is working across various IRS organizations to define disciplined processes for software requirements management, quality assurance, configuration management, and project planning and tracking. In addition, on May 15, 1997, IRS issued for comment a technical architecture for the modernization. Further, IRS has prepared a schedule for implementing our recommendations and has provided it to the Congress.

While we are encouraged by IRS' and Treasury's actions, we remain concerned that continued progress is necessary to fully implement essential improvements. First, increasing the use of contractors will not automatically increase the likelihood of successful modernization because IRS does not have the disciplined acquisition processes needed to manage all of its current contractors. As a case in point, IRS' Cyberfile–a system development effort led by contractors to enable taxpayers to personally prepare and file their tax returns electronically–exhibited many undisciplined software acquisition practices as well as inadequate financial and management controls. Eventually, IRS canceled the Cyberfile project after spending over $17 million and without fielding any of the system's promised capabilities. Therefore, if IRS is to use additional contractors effectively, it will have to first strengthen and improve its ability to manage those contractors.

In addition, IRS needs to continue to make concerted, sustained efforts to fully implement our recommendations and respond effectively to the requirements outlined by the Congress. It will take both management commitment and technical discipline for IRS to do this effectively. Accordingly, we plan to continue assessing IRS' progress in its critical endeavor to modernize.

Question: Doctor Stillman, what should we do about the TSM project? Should we continue to provide funding? What would happen to the nation's collection systems if we were to call a halt to the modernization efforts?

GAO Response: As we noted in our recent high-risk reports addressing TSM,[4] IRS needs to continue to make concerted, sustained efforts to fully implement our recommendations and respond to the requirements outlined by the Congress. These efforts should include (1) limiting information system projects, both in house and contracted out, to small, low risk, near-term projects that IRS has the ability to successfully develop or acquire, (2) improving IRS' system development and acquisition capabilities, (3) finalizing the architecture and ensuring that all IRS system projects conform to it, (4) instituting disciplined investment processes to ensure that all information technology investment decisions (e.g., project selection, control, and evaluation) are based on reliable, objective, and, whenever possible, quantitative data including cost and risk adjusted return on investment, (5) reengineering IRS business processes, focusing on electronic filing, and using these improved processes to determine those information technology investments needed to support the new processes, and (6) ensuring that all future IRS information systems budgets take into account IRS' performance as specified in the Clinger-Cohen Act.

These efforts will take both management commitment, follow-through, and technical discipline by IRS in partnership with the Treasury Department, OMB, and the Congress. Once these essential improvements are made, IRS should have an effective implementation strategy for achieving its business vision, the capacity to make sound investments in information technology, and the necessary technical foundation for effectively modernizing its processes and systems.

However, until these essential improvements are made and adequate justifications for system investments provided, the Congress, as we suggested in June and September 1996,[5] could continue to limit modernization funding to only cost-effective efforts that (1) support ongoing operations and maintenance, (2) correct IRS' pervasive management and technical weaknesses, (3) are small, represent low technical risk, and can be delivered quickly, and (4) involve deploying already developed systems, only if these systems have been fully tested, are not premature given the lack of a completed architecture, and produce a proven, verifiable business value. As the Congress gains confidence in IRS' ability to successfully develop these smaller, cheaper, quicker projects, it could consider approving larger, more complex, more expensive projects in future years.

---

[4]High-Risk Series: IRS Management (GAO/HR-97-8, February 1997) and High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

[5]Tax Systems Modernization: Actions Underway But Management and Technical Weaknesses Not Yet Corrected (GAO/T-AIMD-96-165, September 10, 1996) and Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses (GAO/AIMD-96-106, June 7, 1996).

Should the Congress completely halt and abandon modernization and IRS continue to maintain its current operational systems and procedures, the Service would continue to collect the vast majority of taxes as it does now through federal tax withholding and deposit processes. IRS' performance in collecting delinquent taxes would probably also remain the same. However, IRS' performance in collecting delinquent taxes, as we have reported,[6] has generally been poor due to IRS' inefficient collection processes and systems.

Question: It has been almost ten years since the 1988 amendments to the Inspector General Act of 1978 placed IRS oversight responsibilities with the Inspector General Office of Treasury and internal audits and inspections with the Office of the Chief Inspector. Do you have any recommendations for improving this level of IRS oversight?

GAO Response: We have not reviewed the responsibilities of Treasury's Office of the Inspector General (OIG), the OIG's role in overseeing IRS, or the roles and responsibilities of IRS' Chief Inspector, and therefore, are not in a position to offer recommendations regarding this level of IRS oversight.

However, our work has addressed the need for Treasury oversight of IRS' modernization activities and identified opportunities for improving this level of oversight. Specifically, since our July 1995 report on the Tax Systems Modernization,[7] Treasury has become more active in overseeing IRS' modernization efforts. In May 1996, Treasury reported to the House and Senate Appropriations Committees on steps under way and planned to exert greater management oversight of IRS' modernization efforts.[8] For example, the department established a Modernization Management Board (MMB), chaired by the Deputy Secretary of the Treasury, to be the primary review and decision-making body for modernization and TSM policy and strategic direction. In addition, Treasury scaled back the overall size of the modernization by approximately $2 billion and is working with IRS to obtain additional contractor help to accomplish the modernization. More recently, the MMB and IRS have reevaluated and terminated selected major modernization development projects, such as the Document Processing System.

---

[6]GAO/HR-97-8, February 1997.

[7]GAO/AIMD-95-156, July 26, 1995.

[8]Report to the House and Senate Appropriations Committees: Progress Report on IRS's Management and Implementation of Tax Systems Modernization, Department of the Treasury, May 6, 1996.

While we recognize Treasury's actions to address IRS problems, much remains to be done to fully implement essential IRS improvements. The department's continued focus on monitoring IRS' corrective actions will be a key factor in ensuring progress.

(511543)

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