United States General Accounting Office

GAO

Testimony

Before the Committee on Governmental Affairs
U.S. Senate

For Release on Delivery
Expected at
9:30 a.m.
Tuesday,
March 26, 1996

TAX SYSTEMS MODERNIZATION

Management and Technical Weaknesses Must Be Overcome To Achieve Success

Statement of Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division

GAO/T-AIMD-96-75

Mr. Chairman and Members of the Subcommittee:

I am pleased to have this opportunity to assist in your review of the Internal Revenue Service's (IRS) Tax Systems Modernization (TSM). Over the past decade, GAO has issued several reports and testified before congressional committees on IRS' costs and difficulties in modernizing its information systems. As a critical information systems project that is vulnerable to schedule delays, cost over-runs, and potential failure to meet mission goals, in February 1995, TSM was added to our list of high-risk areas.[1]

IRS invested about $2.5 billion in TSM from 1986 through the end of fiscal year 1995. In addition, it plans to spend an additional $695 million for fiscal year 1996 for this effort, and through 2001, it is expected to spend up to $8 billion on TSM. By any measure, this is a world-class information systems development effort, much larger than most other organizations will ever undertake. TSM is key to IRS' vision of a virtually paper-free work environment where taxpayer account updates are rapid, and taxpayer information is readily available to IRS employees to respond to taxpayer inquiries.

IRS recognizes the criticality to future efficient and effective operations of attaining its vision of modernized tax processing, and has worked for almost a decade, with substantial investment, to reach this goal. In doing so, IRS has progressed in many actions that were initiated to improve management of information systems; enhance its software development capability; and better define, perform, and manage TSM's technical activities. However, this effort to modernize tax processing is jeopardized by persistent and pervasive management and technical weaknesses.

In July 1995, we reported on these weaknesses and made over a dozen specific recommendations which were intended to correct many of these weaknesses by December 31, 1995.[2] IRS has initiated some activities to address these weaknesses. However, as we reported earlier this month, none of these activities, either individually or in the aggregate, has fully satisfied any of our recommendations.[3] Further, ongoing efforts do not provide enough evidence that weaknesses will soon be corrected. As a

[1]High-Risk Series: An Overview (GAO/HR-95-1, February 1995).

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

[3]Status of Tax Systems Modernization, Tax Delinquencies, and the Potential for Return-free Filing (GAO/T-GGD/AIMD-96-88, March 14, 1996).

result, IRS continues with plans to spend billions more on TSM with little assurance of successfully delivering effective systems within established time frames and cost figures.

As you requested, my statement today will address (1) IRS' efforts to correct management and technical weaknesses that have impeded its TSM program and (2) analogous technical weaknesses in the recent Cyberfile effort, indicating that IRS is continuing to risk millions of dollars in undisciplined systems development. Cyberfile, which is planned to allow taxpayers to submit their returns electronically from personal computers, is being developed for the IRS by the Department of Commerce's National Technical Information Service (NTIS) at an estimated cost of $22 million.

While our work on Cyberfile in response to the Chairman's February 1996 request is still continuing, I will also outline some contractual issues that warrant further review. Additionally, as you requested, I have also included a discussion of our fiscal year 1994 financial audit of the IRS—our most recently completed audit.

Pervasive TSM Management and Technical Weaknesses Have Not Been Corrected

Modernizing tax processing is key to IRS' vision of a virtually paper-free work environment in which taxpayer information is readily available to IRS employees to update taxpayer accounts and respond to taxpayer inquiries. In our July 1995 report, we emphasized the need for IRS to have in place sound management and technical practices to increase the likelihood that TSM's objectives will be cost-effectively and expeditiously met.[4] A 1996 National Research Council report on TSM has a similar message.[5] Its recommendations parallel the recommendations we made involving IRS' (1) business strategy to reduce reliance on paper, (2) strategic information management practices, (3) software development capabilities, (4) technical infrastructures, and (5) organizational controls.

The Treasury, Postal Service and General Government Appropriations Act, 1996 "fences" $100 million in TSM funding for fiscal year 1996 until the Secretary of the Treasury reports to the Senate and House Appropriations Committees on the progress IRS has made in responding to our recommendations with a schedule for successfully mitigating deficiencies

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

[5]Continued Review of the Tax Systems Modernization of the Internal Revenue Service—Final Report, Computer Science and Telecommunications Board, National Research Council, 1996.

we reported.[6] The conference report on the act directed that GAO assess for the Committee the status of IRS' corrective actions.[7] As of March 22, 1996, the Secretary of the Treasury had not submitted a report responding to our recommendations to the Committees.

In our July report, we analyzed IRS' strategic information management practices, drawing heavily from our research on the best practices of private and public sector organizations that have been successful in improving their performance through strategic information management and technology. These fundamental best practices are discussed in our report Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology (GAO/AIMD-94-115, May 1994), and our Strategic Information Management (SIM) Self-Assessment Toolkit (GAO/Version 1.0, October 28, 1994, exposure draft). In this regard, our work in this area has been of particular interest to this Committee in its recent efforts to reauthorize the Paperwork Reduction Act and initiate the Information Technology Management Reform Act to require federal agencies to use these modern management practices to improve the federal government's efforts to successfully use information technology to enhance its performance and reduce costs.

To evaluate IRS' software development capability, we validated IRS' August 1993 assessment of its software development maturity based on the Capability Maturity Model (CMM) developed in 1984 by Carnegie Mellon University's Software Engineering Institute, a nationally recognized authority in the area. This model establishes standards in key software development processing areas (i.e., requirements management, project planning, project tracking and oversight, configuration management, quality assurance, and subcontractor management) and provides a framework to evaluate a software organization's capability to consistently and predictably produce high-quality products.

When we briefed the IRS Commissioner in April 1995 and issued our report documenting its weaknesses in July 1995, IRS agreed with our recommendations to make corrections expeditiously. At that time, we considered IRS' response to be a commitment to correct its management and technical weaknesses. In September 1995, IRS submitted an action plan to the Congress explaining how it planned to address our recommendations. However, this plan, follow-up meetings with senior IRS officials, and other draft and "preliminary draft" documents received

[6]Public Law 104-52, 11-19-95.

[7]H.R. Report No. 291, 104th Cong., 1st Session (1995).

through early March 1996 have provided little tangible evidence that actions being taken will correct the pervasive management and technical weaknesses that continue to place TSM, and the huge investment it represents, at risk.

Our ongoing assessment has found that IRS has initiated a number of activities and made some progress in addressing our recommendations to improve management of information systems; enhance its software development capability; and better define, perform, and manage TSM's technical activities. However, none of these steps has fully satisfied any of our recommendations. Consequently, IRS today is not in an appreciably better position than it was a year ago to ensure the Congress that it will spend its 1996 and future TSM appropriations judiciously and effectively.

IRS Still Does Not Have a Comprehensive Strategy to Maximize Electronic Filings

We reported that IRS was drowning in paper—a serious problem IRS can mitigate only through electronic tax filings. We noted that IRS would not achieve the full benefits that electronic filing can provide because it did not have a comprehensive business strategy to reach or exceed its electronic filing goal, which was 80 million electronic filings by 2001. IRS' estimates and projections for individual and business returns suggested that, by 2001, as few as 39 million returns may be submitted electronically, less than half of IRS' goal and only about 17 percent of all returns expected to be filed.

We reported that IRS' business strategy would not maximize electronic filings because it primarily targeted taxpayers who use a third party to prepare and/or transmit simple returns, are willing to pay a fee to file their returns electronically, and are expecting refunds. Focusing on this limited taxpaying population overlooked most taxpayers, including those who prepare their own tax returns using personal computers, have more complicated returns, owe tax balances, and/or are not willing to pay a fee to a third party to file a return electronically.

We concluded that, without a strategy that also targets these taxpayers, IRS would not meet its electronic filing goals or realize its paperless tax processing vision. In addition, if, in the future, taxpayers file more paper returns than IRS expects, added stress will be placed on IRS' paper-based systems. Accordingly, we recommended that IRS

refocus its electronic filing business strategy to target, through aggressive marketing and education, those sectors of the taxpaying population that can file electronically most cost-beneficially.

IRS agreed with this recommendation and said that it had convened a working group to develop a detailed, comprehensive strategy to broaden public access to electronic filing, while also providing more incentives for practitioners and the public to file electronically. It said that the strategy would include approaches for taxpayers who are unwilling to pay for tax preparer and transmitter services, who owe IRS for balances due, and/or who file complex tax returns. IRS said further that the strategy would address that segment of the taxpaying population that would prefer to file from home, using personal computers.

Since then, IRS has performed an electronic filing marketing analysis at local levels; developed a marketing plan to promote electronic filing; consolidated 21 electronic filing initiatives into its Electronic Filing Strategies portfolio; and initiated a reengineering project to begin this month with a goal to reduce paper tax return filings to 20 percent or less of the total volume by 2000. These initiatives could result in future progress toward increasing electronic filings. However, these initiatives have yet to culminate in a comprehensive strategy that identifies how IRS plans to target those sectors of the taxpaying population that can file electronically most cost-beneficially, and what efforts it will make to develop requisite supporting systems.

IRS' Strategic Information Management Practices Remain Ineffective

We reported that IRS did not have strategic information management practices in place. We found, for example, that, despite the billions of dollars at stake, information systems were not managed as investments. To overcome this, and provide the Congress with insight needed to assess IRS' priorities and rationalization for TSM projects, we recommended that the IRS Commissioner

take immediate action to implement a complete process for selecting, prioritizing, controlling, and evaluating the progress and performance of all major information systems investments, both new and ongoing, including explicit decision criteria, and

using these criteria, to review all planned and ongoing systems investments by June 30, 1995.

In agreeing with these recommendations, IRS said it would take a number of actions to provide the underpinning it needs for strategic information management. IRS said, for example, that it was developing and implementing a process to select, prioritize, control, and evaluate information technology investments to achieve reengineered program missions.

Since then, IRS has taken steps towards putting into place a process for managing its extensive investments in information systems. For example, IRS has created the executive-level Investment Review Board for selecting, controlling, and evaluating all information technology investments; developed initial and revised sets of decision criteria that it used last summer to rank and prioritize TSM projects and used it in November 1995 to recommend additional changes to information systems resource allocations, respectively; developed its Investment Evaluation Handbook and Business Case Handbook to strengthen management decision-making on systems investments; and is using the Investment Evaluation Handbook to review operational TSM projects.

Although these steps represent some progress in responding to our concerns, IRS has not demonstrated that it is following a well-defined, consistent, and repeatable information technology investment decision-making process for selecting, controlling, and evaluating its information technology initiatives and projects. In particular, working procedures, required decision documents, decision criteria, and reliable cost, benefit and return data needed for an investment process are not complete. IRS has not provided evidence to demonstrate how analyses are being conducted on all systems investments using such data as expected improvement in mission performance, costs to date, technical soundness, or pilot performance. Instead, IRS operates on the assumption that it will receive a specified funding ceiling for systems development and technology, and then determines how much funding can be eliminated from projects in order to lower overall modernization costs to that level.

Over the last few months, we have communicated several concerns to IRS about weaknesses with its current investment process that continue to raise risks and erode confidence in the quality of decisions being made about TSM investments. These include:

- the absence of initial screening criteria to determine if IRS has developed sufficient data about an information technology project—such as benefit-cost analyses, proposed return-on-investment calculations, and an

accepted return on investment threshold level used as a decisional cut-off point—in order for the investment review board to reach an informed funding decision;
- the lack of analysis and trade-offs being made among all proposed information technology investments as a single portfolio—such as spending on legacy, infrastructure, and proposed modernization projects—in order to fully justify a ranking and prioritization of modernization efforts; and
- the lack of mechanisms to assure that the results of IRS' investment evaluation reviews, such as that recently completed on the Service Center Recognition/Image Processing System, are being used to modify selection and control decision-making processes or to change funding decisions for projects.

Software Development Activities Are Still Inconsistent and Poorly Controlled

We reported that unless IRS improves its software development capability, it is unlikely to build TSM timely or economically, and systems are unlikely to perform as intended. To assess its software capability, in September 1993, IRS rated itself using the Software Engineering Institute's CMM. IRS found that, even though TSM is a world-class undertaking, its software development capability was immature.

IRS placed its software development capability at the lowest level, described as ad hoc and sometimes chaotic and indicating significant weaknesses in its software development capability. Our review also found that IRS' software development capability was immature and was weak in key process areas. For instance,

- a disciplined process to manage system requirements was not being applied to TSM systems,
- a software tool for planning and tracking development projects was not consistently used,
- software quality assurance functions were not well defined or consistently implemented,
- systems and acceptance testing were neither well defined nor required, and
- software configuration management[8] was incomplete.

[8]Configuration management involves selecting project baseline items (e.g., specifications), systematically controlling these items and changes to them, and recording their status and changes.

To address IRS' software development weaknesses and upgrade IRS' software development capabilities, we recommended that the IRS Commissioner

immediately require that all future contractors who develop software for the agency have a software development capability rating of at least CMM level 2,[9] *and*

before December 31, 1995,

define, implement, and enforce a consistent set of requirements management procedures for all TSM projects that goes beyond IRS' current request for information services process, and for software quality assurance, software configuration management, and project planning and tracking; and

define and implement a set of software development metrics to measure software attributes related to business goals.

IRS agreed with these recommendations and said that it was committed to developing consistent procedures addressing requirements management, software quality assurance, software configuration management, and project planning and tracking. Regarding metrics, IRS said that it was developing a comprehensive measurement plan to link process outputs to external requirements, corporate goals, and recognized industry standards.

Specifically regarding the first recommendation, IRS has (1) developed standard wording for use in new and existing contracts that have a significant software development component, requiring that all software development be done by an organization that is at CMM Level 2, (2) developed a plan for achieving CMM Level 2 capability on all of its contracts, and (3) initiated plans for acquiring expertise for conducting CMM-based software capability evaluations of contractors and has designated personnel to perform these evaluations. We found, however, no evidence that all contractors developing software for the agency are being required to develop it at CMM Level 2. For example, our review of the

[9]The Software Engineering Institute at Carnegie Mellon University has developed a model, the Software Capability Maturity Model (CMM), to evaluate an organization's software development capability. CMM level 2 denotes that basic project management processes are established to track cost, schedule, and functionality and the necessary process discipline is in place to repeat earlier successes on similar projects.

Cyberfile electronic filing system being developed by NTIS and contractors found that the system was not being developed at CMM Level 2.

With respect to the second recommendation, IRS is updating three software development lifecycle methodologies, developed a draft quality audit procedures handbook, updated its requirements management request for information services document, and developed and implemented a requirements management course. IRS also evaluated its current contractor management processes, compared these processes to the CMM goals, and is considering improvement activities.

However, to progress towards CMM Level 2, IRS must do a better job to define and implement detailed procedures for the key process areas and allocate the necessary resources. Until this occurs, IRS software development projects will continue to be built using ad-hoc and chaotic processes that offer no assurance of successful delivery.

Since our review IRS has also started a three-phase process to (1) identify data sources for metrics, (2) define metrics to be used, and (3) implement the metrics. According to IRS, although phase one has been completed, no metrics have been defined, and implementation is currently planned for sometime between June 1996 and January 1997. In this regard, although IRS has begun to act on our recommendations, systems are still being developed without the data and discipline needed to give management assurance that they will perform as intended.

Systems Architectures, Integration, and Testing Continue to Be Inadequate

We reported that IRS' systems architectures,[10] integration planning, and system testing and test planning were incomplete. To address IRS' technical infrastructure weaknesses, we recommended that the IRS Commissioner

before December 31, 1995,

complete an integrated systems architecture, including security, telecommunications, network management, and data management;

[10]A system architecture is an evolving description of an approach to achieving a desired mission. It describes (1) all functional activities to be performed to achieve the desired mission, (2) the system elements needed to perform the functions, (3) the designation of performance levels of those system elements, and (4) the technologies, interfaces, and location of functions.

institutionalize formal configuration management for all newly approved projects and upgrades and develop a plan to bring ongoing projects under formal configuration management;

develop security concept of operations, disaster recovery, and contingency plans for the modernization vision and ensure that these requirements are addressed when developing information system projects;

develop a testing and evaluation master plan for the modernization;

establish an integration testing and control facility; and

complete the modernization integration plan and ensure that projects are monitored for compliance with modernization architectures.

IRS agreed with these recommendations and said that it was identifying the necessary actions to define and enforce systems development standards and architectures agencywide. IRS' current efforts in this area follow:

- IRS is developing a "descriptive overview" of an integrated systems architecture, which, for example, includes a security architecture chapter. A draft of the descriptive overview is due in April 1996 and an executive summary is due in mid-March.
- IRS has developed and distributed a Configuration Management Plan template, which identifies the elements needed when constructing a configuration management plan, and established a charter for its Configuration Management branch.
- IRS has prepared a security concept of operations and a disaster recovery and contingency plan.
- IRS has developed a test and evaluation master plan for TSM.
- IRS is in the process of establishing an interim integration testing and control facility but has not determined an initial operating date. It is also planning a permanent integration testing and control facility, scheduled to be completed by the end of 1996.
- IRS has completed an informal draft of its TSM Release Definition Document and a draft of its Modernization Integration Plan.

These activities start to address our recommendations. However, they do not fully satisfy any of our recommendations for the following reasons.

First, IRS has not completed an integrated systems architecture (the "blueprints" of TSM), and no evidence has been provided to suggest that it will have one in the foreseeable future. The draft architecture documents received are high-level descriptions that fall far short of the level of detail needed to provide effective guidance in designing and building systems. For example, IRS' concept of a three-tier, distributed architecture does not provide sufficient detail to understand the security requirements and implications. It does not, for instance, specify what security mechanisms are to be implemented between and among the three tiers to ensure that only properly authorized users are allowed to access tax processing application software and taxpayer data.

Second, IRS has not brought its development, acceptance, and production environments under configuration management control. For example, there is no disciplined process for moving software from the test to the production environment.

Third, our review of the security concept of operations found that the document does not identify selected security methods and techniques. For example, it discusses two methods for providing identification and authentication for controlling user access to various systems without specifying which method should be used. The security concept of operations is also sometimes inconsistent with the security mechanisms currently being implemented on systems now being developed and does not indicate how, when, or if these inconsistencies will be resolved.

Fourth, IRS' disaster recovery and contingency plan is a high-level document for planning that presents basic tenets for information technology disaster recovery but not the detail needed to provide guidance. For example, it does not explain the steps that computing centers need to take to absorb the workload of a center that suffers a disaster.

Fifth, the test and evaluation master plan provides the guidance needed to ensure sufficient developmental and operational testing of TSM. However, it does not describe what security testing should be performed, or how these tests should be conducted. Further, it does not specify the responsibilities and processes for documenting, monitoring, and correcting testing and integration errors.

Sixth, the plans for IRS' integration testing and control facility are inadequate. The purpose of an off-line test site is to provide a safe,

controlled environment for testing that realistically simulates the production environment. This permits new hardware and software to be thoroughly tested without putting IRS operations and service to taxpayers at risk. However, current plans for the facility do not provide for the testing of all IRS software prior to nationwide delivery. It is unclear why this position has been taken or how difficult and expensive it will be to make the modifications needed to enable the facility to effectively replicate its operational environment.

Finally, IRS' draft TSM Release Definition Document and Modernization Integration Plan have not been finalized. In addition, they (1) do not reflect TSM rescoping and the information systems reorganization under the Associate Commissioner, (2) do not provide clear and concise links to other key documents (e.g., its integrated systems architecture, business master plan, concept of operations, and budget), and (3) assume that IRS has critical processes in place that are not implemented (e.g., effective quality assurance and disciplined configuration management).

No Single Entity Controls All Information Systems Efforts

We reported that IRS had not established an effective organizational structure to consistently manage and control systems modernization organizationwide. The accountability and responsibility for IRS' systems development was spread among IRS' Modernization Executive, Chief Information Officer, and research and development division. To help address this concern, in May 1995, the Modernization Executive was named Associate Commissioner. The Associate Commissioner was to manage and control systems development efforts previously conducted by the Modernization Executive and the Chief Information Officer.

In September 1995, the Associate Commissioner for Modernization assumed responsibility for the formulation, allocation, and management of all information systems resources for both TSM and non-TSM expenditures. In February 1996, IRS issued a Memorandum of Understanding providing guidance for initiating and conducting technology research and for transitioning technology research initiatives into system development projects.

It is important that IRS maintain an organizationwide focus to manage and control all new modernization systems and all upgrades and replacements of operational systems throughout IRS. To fully strengthen systems development accountability and responsibility, we recommended that the IRS Commissioner

give the Associate Commissioner management and control responsibility for all systems development activities, including those of IRS' research and development division.

We are concerned that IRS still has not established an organizationwide focus to consistently manage and control information systems. Specifically, we have seen no evidence that systems development, upgrades, and replacements at IRS field locations are being controlled by the Associate Commissioner. Although the Associate Commissioner was given authority for the formulation, allocation, and management of all information systems resources for TSM and non-TSM systems, the research and development division still retains approval authority for initiating technology research projects and for conducting proof-of-concept systems prototypes. It is unclear whether the building processes and budget used for these systems development areas are controlled by the Associate Commissioner.

Again, despite some improvements in consolidating management control over systems development, IRS still does not have a single entity with the responsibility and authority to control all of its information systems projects.

Cyberfile Development Exhibits Many of the Same Technical Weaknesses Identified in TSM

IRS began developing Cyberfile in mid-1995 to allow taxpayers to prepare and electronically submit their tax returns using their personal computers without having to pay a transmission fee. NTIS through an interagency agreement with IRS is developing and planning to operate Cyberfile in a new NTIS data center. Cyberfile is planned to accept tax returns submitted via the public switch telephone network and the Internet. When tax returns are accepted by Cyberfile, they will be forwarded to designated IRS Service Centers.

In December 1995, we briefed the IRS Commissioner on the risks associated with using Cyberfile. At that time, Cyberfile development was scheduled for limited operational use by a selected population of taxpayers in February 1996. Earlier this month, IRS decided to delay Cyberfile operations to an unspecified date after April 15, 1996.

Our review of the Cyberfile development reflects many of the management and technical weaknesses we identified in our July 1995 report. Specifically, Cyberfile is not being developed (1) using disciplined systems

development processes and (2) to provide the security needed to protect taxpayer data.

Disciplined Systems Development Processes Not Used

To increase the likelihood of successful systems development efforts, our July 1995 report recommended that IRS require that all systems procured from contractors be built using disciplined, repeatable CMM level 2 processes as defined by the Software Engineering Institute. Although IRS agreed with this recommendation, it did not stipulate these requirements for Cyberfile.

As a result, by February 29, 1996, IRS had committed about $17 million to NTIS to acquire hardware, software, and telecommunications services for Cyberfile and NTIS had obligated $11.7 million, but the Cyberfile system development effort exhibited many of the same technical weaknesses that we found in TSM. Because IRS did not require that contractors use at least CMM level 2's disciplined software development processes, there was little assurance that Cyberfile would perform as intended and would be delivered on time and within budget.

Because these disciplined processes were not established for Cyberfile's development, the following are examples of the weakness that occurred.

(1) There is no formal process in place to define, manage, and control Cyberfile requirements.

(2) Key planning documents, such as a detailed business plan, security architecture, and concept of operations, have not been completed.

(3) IRS did not perform an alternatives analysis to identify various feasible solutions and their associated costs and benefits.

(4) IRS did not perform a thorough risk analyses to determine the severity of vulnerabilities and the costs associated with mitigating these vulnerabilities.

(5) We were provided no evidence that IRS followed our recommendation to use formal methods or tools to either estimate, plan, or track this TSM development activity. As a result, estimates of Cyberfile cost, performance, and schedule are not based on objective, explicit source data, established methodology, or documented rationale.

In addition, we found that Cyberfile project planning was schedule, rather than event, driven. For example, IRS planned to make a decision on operating Cyberfile as early in this tax filing season as January 1996, even though key requirements and design prerequisites like a security policy, security architecture, test plans, and penetration testing[11] had not yet been completed.

IRS' reasons for continuing plans to operate Cyberfile during the current tax filing season are unclear. A November 1995, market study performed for IRS projected that of an estimated 4 million taxpayers who would be eligible for the Cyberfile project, 10,000 to 25,000 taxpayers would likely have used Cyberfile if it had been operational throughout the current tax filing season. Because operations have been delayed beyond April 15, it is unclear what benefits IRS expects to be derived from rushing to operate Cyberfile this year. In this regard, IRS' market study noted that past patterns of electronic filings have shown that, very few taxpayers file electronically after April 15.

Cyberfile Security Is Inadequate

System security requirements provide systems developers with the "blueprints" needed to ensure that systems being developed will adequately protect the data and access to the data. Our July 1995 recommendations were intended to ensure that security requirements for sensitive systems like Cyberfile would be addressed.

Federal Information Processing Standards define among other things, approved techniques that can be used to authenticate users and ensure data privacy, integrity, and nonrepudiation.[12] In an April 1995 proposal from NTIS to IRS to conduct an analysis and feasibility study, these security requirements were identified at a conceptual level. However, subsequent system documentation and action taken did not address these issues in accordance with Federal Information Processing Standards. For instance, the April 1995 proposal cited the requirement for a digital signature, but succeeding documentation describes a system using a personal electronic filing number, which will not ensure data integrity or nonrepudiation. We were provided no documented rationale for these changes in

[11]Penetration testing is a testing activity that, by attempting to break into a computer network or system exposes security flaws and weaknesses.

[12]In a system that ensures nonrepudiation, effective controls are in place to preclude users from later denying that they sent the signed messages.

requirements, or for other security related decisions, such as the choice of encryption approaches[13] and security products like fire walls.[14]

Significant Physical Security Risks Exist for Cyberfile

On March 12, 1996, we toured and assessed Cyberfile's data center, which according to data center management was scheduled to be operationally ready on March 19, 1996. Our review of 7 functional areas found that many controls, which should have been in place by this time to mitigate security-related risks, were not. Specifically, we reviewed (1) data center operations, (2) physical security, (3) data communications management, (4) disaster recovery, (5) contingency planning, (6) risk analysis, and (7) security awareness. We found weaknesses in all seven areas.

Data Center Operations

Effective data center operations include strong operational security safeguards to assure the continuity of operations. We found 17 operational security weaknesses in a dusty construction environment that place the equipment at operational risk. The following are examples of these weaknesses.

- Large amounts of combustible materials were found adjacent to and inside the data center. Paper and cardboard trash was piled in adjacent areas, and boxes of envelopes were stacked in the data center.
- The data center's fire extinguishers required recharging and were haphazardly placed in the center, increasing vulnerability to extensive fire damage.
- The center uses wet standpipe sprinklers for fire suppression in lower than normal ceilings. Taller individuals in the center have to duck to avoid hitting the sprinklers, which, if inadvertently sheared off, will release water that can damage the center.
- The data center is located on the subbasement level of a building and does not have water detectors under the raised floor, increasing the risk of extensive electrical damage to computer equipment if the center floods.

Physical Security

Physical security and access control measures, such as locks, guards, and surveillance cameras are critical to safeguarding data and operations from internal and external threats. At the data center we found 14 physical security weaknesses, including the following.

[13]Encryption is the process of scrambling information to make it unreadable to protect it from unauthorized viewing or use.

[14]Firewalls are computer systems designed to protect specified computer resources, like Cyberfile, from outside network users, like Internet users.

- The lock on the main door to the data center was improperly installed, exposing the mechanism and permitting unauthorized access by just flipping the latch with a finger.
- All doors to the data had unsecured hinges on the outside, allowing easy removal of doors to permit unauthorized entrance to the data center.
- Multiple exit doors were not alarmed or monitored by security cameras, thereby allowing exit and entrance without detection.
- Packages and other personal articles were not inspected before being allowed in the data center, increasing internal security threats. This leaves the center vulnerable to physical attack from concealed weapons, as well as technical attack. For example, malicious software could be brought in to introduce viruses.
- Electronic card key devices installed on doors in an environment without guards or cameras do not limit access to authorized personnel only. Unauthorized personnel can follow cardholders into the center and pose a threat to the equipment and taxpayer data.

Data Communications Management

Data communications management is the function of monitoring and controlling communications networks to ensure that they operate as intended, transmitting timely, accurate, and reliable data in a secure fashion to and from taxpayers. We found 10 communications management weaknesses at Cyberfile's data center. For example, telecommunications equipment such as telecommunication switches and patch panels was not physically protected and could be accessed and damaged by unauthorized personnel. Additionally, communications devices intended to be used only to monitor data flow can also be used to alter data and for browsing.

Disaster Recovery

Effective disaster recovery plans and procedures enable organizations to continue operations or to reestablish operations in a backup facility after disruptions caused by events such as earthquakes, floods, fires, and electrical power failures. Cyberfile does not have a backup computer facility, nor does it have alternate power sources to maintain computer operations during a power outages.

Contingency Planning

Contingency planning provides specific procedures that need to be taken during various emergencies to restore critical operations and identifies the key individuals responsible for carrying out the procedures. While NTIS has a draft contingency plan that provides some high level instructions on maintaining continuous Cyberfile system operations, the draft does not have specific procedures to be followed in an emergency nor does it identify the key individuals responsible for carrying them out.

Risk Analysis

A risk analysis identifies and determines the severity of security threats and, for each threat, formulates safeguards, and estimates their cost. The risk analysis conducted for Cyberfile was incomplete and did not adequately address physical, operational, and communications security threats to the data center. For example, the analysis does not address the threat of data center employees compromising taxpayer data. Without a comprehensive risk analysis, system vulnerabilities may not be identified and cost effective controls may not be implemented to mitigate them.

Security Awareness

A security awareness program communicates to employees the importance of security measures and emphasizes their responsibility for protecting assets. We found that there was no security awareness program for Cyberfile. During our review, we found a note, written on a white board in the data center, instructing employees to handoff passwords to employees on the next shift. Because employees share passwords, system and data accesses and the use of system resources cannot be traced to individuals, and, therefore, cannot be effectively controlled.

Cyberfile Contractual Issues Warrant Further Review

Our review of the acquisition process raised several issues that warrant further explanation by IRS or NTIS. In this regard, we plan to review these issues during our continuing review of Cyberfile.

NTIS implemented its interagency agreement with IRS chiefly through means of a contract awarded to a contractor under the "Section 8(a)" program. The "Section 8(a)" program permits the award of a contract to the Small Business Administration, which then subcontracts with a firm owned by economically and socially disadvantaged individuals. This type of contract can be awarded with limited or no competition. In this case, NTIS awarded a contract under "Section 8(a)" on a sole source basis. The selected contractor then subcontracted a significant part of its work to other firms. Information obtained indicates that the selection of some of these subcontractors may have been directed by NTIS or IRS. These actions may have resulted in the complete elimination of competition for a significant amount of government business.

Also, numerous actions were conducted quickly and information obtained to date does not provide a clear understanding of what transpired. For example, in rushing to implement Cyberfile, it appears that IRS contracted for services that NTIS was tasked with providing under their interagency agreement. In addition, procurement officials at both IRS and Commerce told us that they believe they followed procurement rules, but said they

received instructions from superiors to proceed with various contracting actions, in some cases without the government receiving the benefit of the traditional independent judgment accorded contracting officials. In this regard, we identified over $2 million in 33 purchases where exemptions to normal purchasing requirements were justified based on 41 U.S.C. 253(c)(2), which states the following.

"The executive agency's need for the property or services is of such an unusual and compelling urgency that the Government would be seriously injured unless the executive agency is permitted to limit the number of sources from which it solicits bids or proposals;"

Our preliminary review of these purchases raises issues concerning the urgency and appropriateness of some of these purchases. For example, four cellular phones were purchased in August 1995, at $1,099 each to provide 24-hour accessibility to key personnel who operate Cyberfile. However, Cyberfile is still not operational and documentation obtained from NTIS indicates that $842 was spent in August and September 1995 on usage charges—with no clear indication on subsequent usage charges. Similar purchases were made for three nationwide pagers costing about $175 each, with documentation indicating that over $4,100 has been budgeted for pager services in 1996. However, as we mentioned earlier more work is needed to assess the appropriateness of all such actions.

Financial Management Weaknesses Persist

Our fiscal year 1994 financial audit of IRS, entitled Financial Audit: Examination of IRS' Fiscal Year 1994 Financial Statements (GAO/AIMD-95-141, August 4, 1995),

(1) highlighted a number of serious managerial problems that IRS must directly address to make greater progress in this area,

(2) discussed actions being taken by IRS to strengthen its operations, and

(3) presented numerous specific GAO recommendations for needed additional improvements.

IRS agreed with all our recommendations and committed itself to taking the corrective measures necessary to improve its financial management operations. We currently are in the process of auditing IRS' fiscal year 1995 financial statements.

For the last 3 fiscal years,[15] we have been unable to express an opinion on IRS' financial statements because of the pervasive nature of its financial management problems. We were unable to express an opinion on IRS' financial statements for fiscal year 1994 for the following five primary reasons.

- One, the amount of total revenue of $1.3 trillion reported in the financial statements could not be verified or reconciled to accounting records maintained for individual taxpayers in the aggregate.
- Two, amounts reported for various types of taxes collected, for example, social security, income, and excise taxes, could also not be substantiated.
- Three, we could not determine from our testing of IRS' gross and net accounts receivable estimates of over $69 billion and $35 billion, respectively, which include delinquent taxes, whether those estimates were reliable.
- Four, IRS continued to be unable to reconcile its Fund Balance With Treasury accounts.
- Five, we could not substantiate a significant portion of IRS' $2.1 billion in nonpayroll expenses included in its total operating expenses of $7.2 billion, primarily because of lack of documentation. However, we could verify that IRS properly accounted for and reported its $5.1 billion of payroll expenses.

To help IRS resolve these issues, we have made dozens of recommendations in our financial audit reports dating back to fiscal year 1992. In total, we have made 59 recommendations on issues covering such areas as tax revenue, administrative costs, and accounts receivable. While IRS has begun to take action on many of our recommendations, as of the date of our last report—August 4, 1995—it had fully implemented only 13 of our 59 recommendations.

IRS has made some progress in responding to the problems we identified in our previous audits. However, IRS needs to intensify its efforts in this area. In a September 12, 1994, letter to the Commissioner, we explained that IRS needed to develop a detailed plan with explicit, measurable goals and a set timetable for action, to attain the level of financial reporting and controls needed to effectively manage its massive operations and to reliably measure its performance. On March 21, 1996, we received a copy of that plan and are now reviewing it.

[15]Financial Audit: Examination of IRS' Fiscal Year 1992 Financial Statements (GAO/AIMD-93-2, June 30, 1993); Financial Audit: Examination of IRS' Fiscal Year 1993 Financial Statements (GAO/AIMD-94-120, June 15, 1994); and Financial Audit: Examination of IRS' Fiscal Year 1994 Financial Statements (GAO/AIMD-95-141, August 4, 1995).

The sections below discuss these issues in greater detail.

Issues With Revenue

IRS' financial statement amounts for revenue, in total and by type of tax, were not derived from its revenue general ledger accounting system (RACS) or its master files of detailed individual taxpayer records. This is because RACS did not contain detailed information by type of tax, such as individual income tax or corporate tax, and the master file cannot summarize the taxpayer information needed to support the amounts identified in RACS. As a result, IRS relied on alternative sources, such as Treasury schedules, to obtain the summary total by type of tax needed for its financial statement presentation.

IRS asserts that the Treasury amounts were derived from IRS records; however, neither IRS nor Treasury's records maintained any detailed information that we could test to verify the accuracy of these figures. As a result, to substantiate the Treasury figures, we attempted to reconcile IRS' master files—the only detailed records available of tax revenue collected—with the Treasury records. We found that IRS' reported total of $1.3 trillion for revenue collections, which was taken from Treasury schedules, was $10.4 billion more than what was recorded in IRS' master files. Because IRS was unable to satisfactorily explain, and we could not determine the reasons for this difference, the full magnitude of the discrepancy remains uncertain.

In addition to the difference in total revenues collected, we also found large discrepancies between information in IRS' master files and the Treasury data used for the various types of taxes reported in IRS' financial statements. Some of the larger reported amounts for which IRS had insufficient support were $615 billion in individual taxes collected—this amount was $10.8 billion more than what was recorded in IRS' master files; $433 billion in social insurance taxes (FICA) collected—this amount was $5 billion less than what was recorded in IRS' master files; and $148 billion in corporate income taxes—this amount was $6.6 billion more than what was recorded in IRS' master files. Thus, IRS did not know and we could not determine if the reported amounts were correct. These discrepancies also further reduce our confidence in the accuracy of the amount of total revenues collected.

Despite these problems, we were able to verify that IRS' reported total revenue collections of $1.3 trillion agreed with tax collection amounts deposited at the Department of the Treasury. However, we did find

$239 million of tax collections recorded in IRS' RACS general ledger that were not included in reported tax collections derived from Treasury data.

In addition to these problems, we could not determine from our testing the reliability of IRS' projected estimate for accounts receivable. As of September 30, 1994, IRS reported an estimate of valid receivables of $69.2 billion,[16] of which $35 billion[17] was deemed collectible. However, in our random statistical sample of accounts receivable items IRS tested, we disagreed with IRS on the validity of 19 percent[18] of the accounts receivable and the collectibility of 17 percent[19] of them. Accordingly, we cannot verify the reasonableness of the accuracy of the reported accounts receivable.

Inadequate internal controls, especially the lack of proper documentation of transactions, resulted in IRS continuing to report unsupported revenue information. In some cases, IRS did not maintain documentation to support reported balances. In other cases, it did not perform adequate analysis, such as reconciling taxpayer transactions to the general ledger, to ensure that reported information was reliable.

We found several internal control problems that contributed to our inability to express an opinion on IRS' financial statements. To illustrate,

- IRS was unable to provide adequate documentation for 111 items, or 68 percent, in our random sample of 163 transactions from IRS' nonmaster file. The nonmaster file is a database of taxpayer transactions that cannot be processed by the two main master files or are in need of close scrutiny by IRS personnel. These transactions relate to tax years dating as far back as the 1960s. During fiscal year 1994, approximately 438,000 transactions valued at $7.3 billion were processed through the nonmaster file. Because of the age of many of these cases, the documentation is believed to have been destroyed or lost.
- We sampled 4,374 statistically projectable transactions posted to taxpayer accounts. However, IRS was unable to provide adequate documentation,

[16]The range of IRS' confidence interval, at a 95-percent confidence level, is that the actual amount of valid accounts receivable as of September 30, 1994, was between $66.1 billion and $72.3 billion.

[17]The range of IRS' confidence interval, at a 95-percent confidence level, is that the actual amount of collectible accounts receivable as of September 30, 1994, was between $34 billion and $36 billion.

[18]The range for our confidence interval, at a 95-percent confidence level, is that the actual amount of the validity exceptions as of September 30, 1994, was between 14.5 percent and 24.2 percent.

[19]The range for our confidence interval, at a 95-percent confidence level, is that the actual amount of the collectibility exceptions as of September 30, 1994, was between 13.1 percent and 22.5 percent.

such as a tax return, for 524 transactions, or 12 percent. Because the documentation was lost, physically destroyed or, by IRS policy, not maintained, some of the transactions supporting reported financial balances could not be substantiated, impairing IRS' ability to research any discrepancies that occur.

- IRS is authorized to offset taxpayer refunds with certain debts due to IRS and other government agencies. Before refunds are generated, IRS policy requires that reviews be performed to determine if the taxpayer has any outstanding debts to be satisfied. For expedited refunds, IRS must manually review various master files to identify outstanding debts. However, out of 358 expedited refunds tested, we identified 10 expedited refunds totaling $173 million where there were outstanding tax debts of $10 million, but IRS did not offset the funds. Thus, funds owed could have been collected but were not.
- IRS could not provide documentation to support $6.5 billion in contingent liabilities reported as of September 30, 1994. Contingent liabilities represent taxpayer claims for refunds of assessed taxes which IRS management considers probable to be paid. These balances are generated from stand-alone systems, other than the master file, that are located in two separate IRS divisions. Because these divisions could not provide a listing of transactions for appropriate analysis, IRS did not know, and we could not determine, the reliability of these balances.
- An area that we identified where the lack of controls could increase the likelihood of loss of assets and possible fraud was in the reversal of refunds. Refunds are reversed when a check is undelivered to a taxpayer, an error is identified, or IRS stops the refund for further review. In many cases, these refunds are subsequently reissued. If the refund was not actually stopped by Treasury, the taxpayer may receive two refunds. In fiscal year 1994, IRS stopped 1.2 million refunds totaling $3.2 billion. For 183 of 244, or 75 percent of our sample of refund reversals, IRS was unable to provide support for who canceled the refund, why it was canceled, and whether Treasury stopped the refund check. Service center personnel informed us that they could determine by a code whether the refund was canceled by an internal IRS process or by the taxpayer, but, as a policy, no authorization support was required, nor did procedures exist requiring verification and documentation that the related refund was not paid.

With regard to controls over the processing of returns, we also found weaknesses. During fiscal year 1994, IRS processed almost 1 billion information documents and 200 million returns. In most cases, IRS processed these returns correctly. However, we found instances where IRS' mishandling of taxpayer information caused additional burden on the

taxpayer and decreased IRS' productivity. In many cases, the additional taxpayer burden resulted from IRS' implementation of certain enforcement programs it uses to ensure taxpayer compliance, one of which is the matching program. This program's problems in timely processing cause additional burden when taxpayers discover 15 months to almost 3 years after the fact that they have misreported their income and must pay additional taxes plus interest and penalties.

Issues With Administrative Operations

IRS has made progress in accounting for its appropriated funds, but there were factors in this area that prevented us from being able to render an opinion. Specifically, IRS was unable to fully reconcile its Fund Balance with Treasury accounts, nor could it substantiate a significant portion of its $2.1 billion in nonpayroll expenses—included in its $7.2 billion of operating expenses—primarily because of lack of documentation.

With regard to its Fund Balance With Treasury, we found that, at the end of fiscal year 1994, unreconciled cash differences netted to $76 million. After we brought this difference to the CFO's attention, an additional $89 million in adjustments were made. These adjustments were attributed to accounting errors dating back as far as 1987 on which no significant action had been taken until our inquiry. IRS was researching the remaining $13 million in net differences to determine the reasons for them. These net differences, which span an 8-year period, although a large portion date from 1994, consisted of $661 million of increases and $674 million of decreases. IRS did not know and we could not determine the financial statement impact or what other problems may become evident if these accounts were properly reconciled.

To deal with its long-standing problems in reconciling its Fund Balance with Treasury accounts, during fiscal year 1994, IRS made over $1.5 billion in unsupported adjustments (it wrote off these amounts) that increased cash by $784 million and decreased cash by $754 million, netting to $30 million. In addition, $44 million of unidentified cash transactions were cleared from cash suspense accounts[20] and included in current year expense accounts because IRS could not determine the cause of the cash differences. These differences suggest that IRS did not have proper controls over cash disbursements as well as cash receipts.

[20]Suspense accounts include those transactions awaiting posting to the appropriate account or those transactions awaiting resolution of unresolved questions.

In addition to its reconciliation problems, we found numerous unsubstantiated amounts. These unsubstantiated amounts occurred because IRS did not have support for when and if certain goods or services were received and, in other instances, IRS had no support at all for the reported expense amount. These unsubstantiated amounts represented about 18 percent of IRS' $2.1 billion in total nonpayroll expenses and about 5 percent of IRS' $7.2 billion in total operating expenses.

Most of IRS' $2.1 billion in nonpayroll related expenses are derived from interagency agreements with other federal agencies to provide goods and services in support of IRS' operations. For example, IRS purchases printing services from the Government Printing Office; phone services, rental space, and motor vehicles from the General Services Administration; and photocopying and records storage from the National Archives and Records Administration.

Not having proper support for if and when goods and services are received made IRS vulnerable to receiving inappropriate interagency charges and other misstatements of its reported operating expenses, without detection. Not knowing if and/or when these items were purchased seriously undermines any effort to provide reliable, consistent cost or performance information on IRS' operations. As a result of these unsubstantiated amounts, IRS has no idea and we could not determine, when and, in some instances, if the goods or services included in its reported operating expenses were correct or received.

Some Improvements Made but Overall Computer Systems Security Remained Weak

In our prior year reports, we stated that IRS' computer security environment was inadequate. Our fiscal year 1994 audit found that IRS had made some progress in addressing and initiating actions to resolve prior years' computer security issues; however, some of the fundamental security weaknesses we previously identified continued to exist in fiscal year 1994.

These weaknesses were primarily IRS' employees' capacity to make unauthorized transactions and activities without detection. IRS has taken some actions to restrict account access, review and monitor user profiles, provide an automated tool to analyze computer usage, and install security resources. However, we found that IRS still lacked sufficient safeguards to prevent or detect unauthorized browsing of taxpayer information and to prevent staff from changing certain computer programs to make unauthorized transactions without detection.

The deficiencies in financial management and internal controls that I have discussed throughout this testimony demonstrate the long-standing, pervasive nature of the weaknesses in IRS' systems and operations—weaknesses which contributed to our inability to express a more positive opinion on IRS' financial statements. The erroneous amounts discussed would not likely have been identified if IRS' financial statements had not been subject to audit. Further, the errors and unsubstantiated amounts highlighted throughout this testimony suggest that information IRS provides during the year is vulnerable to errors and uncertainties as to its completeness and that reported amounts may not be representative of IRS' actual operations.

IRS Has Taken Steps to Improve Its Financial Operations

IRS has made some progress in responding to the problems we have identified in previous reports. It has acknowledged these problems, and the Commissioner has committed to resolving them. These actions represent a good start in IRS' efforts to more fully account for its operating expenses. For example, IRS has

- successfully implemented a financial management system for its appropriated funds to account for its day-to-day operations, which should help IRS to correct some of its past transaction processing problems that diminished the accuracy and reliability of its cost information; and
- successfully transferred its payroll processing to the Department of Agriculture's National Finance Center and, as a result, properly accounted for and reported its $5.1 billion of payroll expenses for fiscal year 1994.

IRS is working on improving the process of reconciling and monitoring its funds. In this regard, it has created a unit whose sole responsibility is to resolve all cash reconciliation issues and retained a contractor to help with this process. In the area of receipt and acceptance, IRS stated that it is more fully integrating its budgetary and management control systems. Also, IRS has developed a methodology to differentiate between financial receivables and compliance assessments and has modified current systems to provide financial management information. Finally, IRS is in the process of identifying methods to ensure the accuracy of balances reported in its custodial receipt accounts. We are currently reviewing these actions as well as the action plan we received from IRS on March 21, 1996.

This concludes my statement. I would be happy to answer any questions you or other members of the Committee may have at this time.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. 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

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