United States General Accounting Office

GAO

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

December 1998

IRS SYSTEMS SECURITY

Although Significant Improvements Made, Tax Processing Operations and Data Still at Serious Risk

GAO/AIMD-99-38

GAO

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

Accounting and Information
Management Division

B-281559

December 14, 1998

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

This report completes our response to your request that we evaluate the Internal Revenue Service's (IRS) progress in correcting the serious computer security weaknesses at five IRS facilities discussed in our April 1997 report on IRS systems security.[1] This report also discusses additional security weaknesses identified at the five facilities and at an IRS facility not included in our previous report, and steps IRS has taken or plans to take to implement a servicewide computer security management program.

On November 30, 1998, we issued to you a report that provides a more detailed discussion of the computer security weaknesses found at IRS facilities. Because some of the weaknesses are sensitive and could jeopardize IRS' security if released to the public, that report is designated "Limited Official Use." We met with IRS officials to obtain their comments in making this report suitable for public release. As a result, this report does not quantify either the total number of weaknesses found or the number of weaknesses found in specific functional categories, and does not detail the most serious weaknesses.

This report restates recommendations made to the Commissioner of Internal Revenue in the "Limited Official Use" version of this report. The Commissioner of Internal Revenue commented on a draft of that report. His comments are discussed in the "Agency Comments and Our Evaluation" section of this report and are reprinted in appendix I.

Results in Brief

IRS is making significant progress to improve computer security over its facilities. Since our April 1997 report, IRS has acknowledged the seriousness of its computer security weaknesses, consolidated overall responsibility for computer security management within one executive-level office under its Chief Information Officer, reevaluated its approach to computer security management, and developed a high-level

[1]IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, April 8, 1997). The report summarized the computer security weaknesses detailed in a "Limited Official Use" report issued in January 1997.

plan for mitigating the weaknesses we identified. We found that IRS has corrected or mitigated the risks associated with 63 percent of the weaknesses discussed in our prior report.

While progress has been made, serious weaknesses continue to exist at the five facilities visited during our prior audit, and we identified several additional weaknesses at those locations and at a sixth facility included in this review. These weaknesses exist primarily because IRS has not yet fully institutionalized its computer security management program. These weaknesses affect IRS' ability to control physical access to its facilities and sensitive computing areas, control electronic access to sensitive taxpayer data and computer programs, prevent and/or detect unauthorized changes to taxpayer data or computer software, and restore essential IRS operations following an emergency or natural disaster. Until these weaknesses are mitigated, IRS continues to run the risk of its tax processing operations being disrupted. Furthermore, sensitive taxpayer data entrusted to IRS could be disclosed to unauthorized individuals, improperly used or modified, or destroyed, thereby exposing taxpayers to loss or damages resulting from identity fraud and other financial crimes.

In comments agreeing with our recommendations, IRS stated that since the end of our review, it had addressed an additional 12 percent of the weaknesses identified. IRS also specified actions planned and underway to address the remaining weaknesses. We will review these actions as part of our audit of IRS' fiscal year 1998 financial statements.

Background

IRS relies on automated information systems to process over 200 million taxpayer returns and collect over $1.6 trillion in taxes annually. IRS uses its computer systems to, among other things, process tax returns, maintain taxpayer data, calculate interest and penalties, and generate refunds. IRS operates facilities throughout the United States that process tax returns and other information supplied by taxpayers. The data are then electronically transmitted to master files of taxpayer information that are maintained and updated. Because of IRS' heavy reliance on its facilities, effective security controls are critical to IRS' ability to maintain the confidentiality of sensitive taxpayer data, safeguard assets, and ensure the reliability of financial management information.

Computer Security Requirements

Federal law, Department of the Treasury directives, and IRS' own internal policies and procedures require the implementation of sound security

practices and standards. The Computer Security Act[2] and the Clinger-Cohen Act[3] require, among other things, the establishment of standards and guidelines for ensuring the security and privacy of sensitive information in federal computer systems. Similarly, IRS' tax information security guidelines require that all computer and communications systems that process, store, or transmit taxpayer data adequately protect these data, and the Internal Revenue Code prohibits the unauthorized disclosure of federal returns and return information outside IRS. To adequately comply with these guidelines, IRS must ensure that (1) access to computer data, systems, and facilities is properly restricted and monitored, (2) changes to computer systems software are properly authorized and tested, (3) backup and recovery plans are prepared, tested, and maintained to ensure continuity of operations in the case of a disaster, and (4) data communications are adequately protected from unauthorized intrusion and interception.

The need for strong and effective computer security over taxpayer information is clear. IRS computer systems contain sensitive taxpayer information such as name, address, social security number, and details on each taxpayer's financial holdings. As we previously reported,[4] these and similar types of information have been used to commit financial crimes and identity fraud nationwide. Commonly reported financial crimes include using someone's personal information to fraudulently establish credit, run up debt, or take over and deplete existing financial accounts. Taxpayers can suffer injury to their reputations when credit is fraudulently established and debts incurred in their names. Bad credit could in turn lead to difficulties in obtaining loans or jobs and require a lengthy and expensive process to clear one's personal records.

Prior GAO Work on IRS Computer Security

Over the past 5 years, we have reviewed the effectiveness of IRS security and general controls as part of our annual audit of IRS' financial statements. During this period, we testified and reported numerous times on the ineffectiveness of these controls in safeguarding IRS computer

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

[3]Public Law 104-106, 110 Stat. 186 (1996).

[4]Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited (GAO/GGD-98-100BR, May 1, 1998).

systems and facilities.[5] In April 1997, we reported on serious weaknesses at five IRS facilities that we visited. These weaknesses were in eight functional areas, which are (1) physical security, (2) logical security,[6] (3) data communications management, (4) risk analysis, (5) quality assurance, (6) internal audit and security,[7] (7) security awareness, and (8) contingency planning. We also noted that IRS' ability to monitor and detect the unauthorized access and perusal of electronic taxpayer records by IRS employees, also known as browsing, was limited. We reported that until these weaknesses are corrected, IRS runs the risk of its tax processing operations being disrupted and taxpayer data being improperly used, modified, or destroyed. Because of the seriousness of the weaknesses, we recommended, among other things, that IRS (1) reevaluate its current approach to computer security and report its plans for improving computer security to the Congress and (2) prepare and submit a plan to the Congress for correcting all the weaknesses identified at the five facilities and for identifying and correcting security weaknesses at the other IRS facilities.

In 1997, the Congress passed the Taxpayer Browsing Protection Act[8] which amended the Internal Revenue Code of 1986 to make unlawful unauthorized access and inspection of taxpayer records a crime and to establish penalties for unlawful access and inspection of taxpayer records.

Objectives, Scope, and Methodology

The objectives of our review were to determine and summarize the status of the computer-related general control weaknesses identified at the five IRS facilities discussed in our April 1997 report and to assess the effectiveness of computer controls at a sixth facility.

To determine the effectiveness of IRS' corrective actions taken to resolve these weaknesses, we interviewed agency officials responsible for correcting them, reviewed these officials' action plans and status reports, and conducted on-site evaluations to verify the effectiveness of corrective actions taken. Our on-site evaluations of IRS computer-related general controls were conducted in conjunction with our audit of IRS' fiscal year

[5]IRS Systems Security: Progress Made to Secure Taxpayer Data But Serious Risk of Improper Access Remains (GAO/AIMD-95-17, December 27, 1994); IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information (GAO/AIMD-93-34, September 22, 1993); and Financial Audit: Examination of IRS' Fiscal Year 1994 Financial Statements GAO/AIMD-95-141, August 4, 1995).

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

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

[8]Public Law 105-35.

1997 custodial financial statements[9] and with the assistance of the independent public accounting firm which also participated in the review supporting our April 1997 report. Our evaluations included the review of related IRS policies and procedures; on-site tests and observations of computer-related controls; and discussions with IRS headquarters and facility personnel, security representatives, and other pertinent officials at the locations visited. Our evaluation did not include external penetration testing of IRS computer facilities.

We performed evaluations at six IRS facilities—the five facilities visited during our previous review and one additional facility. We requested and received IRS comments on the results of our on-site evaluations from the Director of the Office of Systems Standards and Evaluation, who has servicewide responsibility for computer security. We did not verify IRS' statements regarding corrective actions taken subsequent to our site visits but plan to do so during future reviews.

To evaluate IRS' computer security management, we assessed information pertaining to computer controls in place at headquarters and field locations and held discussions with headquarters officials. We did not assess the computer-related controls that IRS plans to incorporate under any of its long-term plans to modernize its tax processing systems. We also did not assess IRS efforts to resolve the Year 2000 computing crisis.

Our work was performed at IRS headquarters in Washington, D.C., and at six facilities located throughout the United States from November 1997 through July 1998. We performed our work in accordance with generally accepted government auditing standards.

IRS Is Taking Action to Improve Security

IRS has taken and is taking action to implement the recommendations contained in our April 1997 report to improve computer security. For example, IRS designated computer security as a material weakness in its fiscal year 1997 Federal Managers' Financial Integrity Act[10] report, acknowledging the seriousness of these computer-related general control weaknesses and the risk they pose to the agency's operations.

[9]Financial Audit: Examination of IRS' Fiscal Year 1997 Custodial Financial Statements (GAO/AIMD-98-77, February 26, 1998).

[10]The Federal Managers' Financial Integrity Act of 1982 (Public Law 97-255) requires the head of each agency to annually prepare a statement that identifies material weaknesses in the agency's systems of internal accounting and administrative control and the plans and schedule for correcting these weaknesses.

IRS Has Consolidated Responsibility for Computer Security

IRS has established the Office of Systems Standards and Evaluation to centralize responsibility for IRS security and privacy issues. The office is staffed with over 60 security, privacy, systems life-cycle, and administrative specialists led by two senior executives who report to the Chief Information Officer. The office is responsible for establishing and enforcing standards and policies for all major security programs including, but not limited to, physical security, data security, and systems security. IRS has acted to address recommendations made in our April 1997 report by

- preparing and transmitting to the Congress a high-level action plan for identifying and correcting the security weaknesses at all of its facilities including the five facilities discussed in our prior report;
- reevaluating and establishing a new approach to managing computer security that involves the resolution of security weaknesses and issues by facility type, including computing centers, service centers, district offices, and others; and
- submitting to the Congress its plan for improving the service's management approach to computer security.

In addition, the Office of Systems Standards and Evaluation has developed computer security awareness briefings on unauthorized access to taxpayers' records, conducted computer security reviews at IRS facilities, and developed a tracking system for reporting the status of actions planned or taken to correct the weaknesses identified in our April 1997 report.

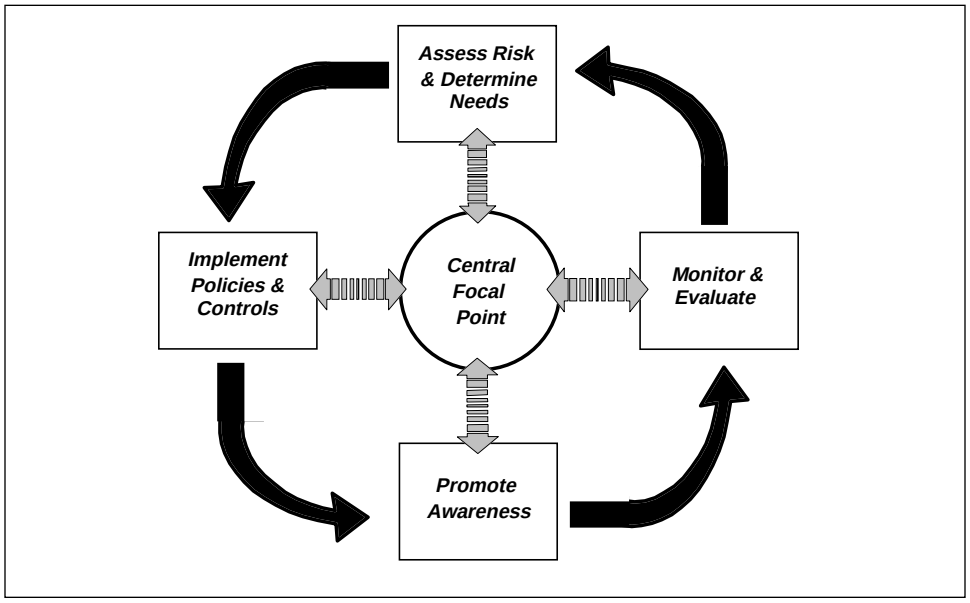
IRS Has Mitigated Many of the Computer Security Weaknesses

We confirmed that IRS has corrected or has implemented compensating controls that mitigated the risks associated with 63 percent of the total weaknesses identified in our April 1997 report. Each facility had varying degrees of success resolving the weaknesses previously reported. The actual rate of resolution ranged from 42 percent to 80 percent. Corrective actions taken by one or more of the five facilities include strengthening the overall controls over physical access to IRS facilities, reducing the number of IRS employees authorized to read or change sensitive system files and/or taxpayer data, conducting risk analyses of the facilities and of locally developed computer programs, updating and testing some disaster recovery plans, and improving overall security awareness.

IRS Has Not Yet Fully Institutionalized Its Servicewide Computer Security Management Program

Although IRS has made significant strides in improving computer security at certain facilities, an effective servicewide computer security management program has not yet been fully implemented. Our study[11] of the security management practices of leading organizations found that these organizations successfully managed their information security risks through an ongoing cycle of risk management activities. As shown in figure 1, each of these activities is linked in a cycle to help ensure that business risks are continually monitored, policies and procedures are regularly updated, and controls are in effect.

Figure 1: Risk Management Cycle



The risk management cycle begins with an assessment of risks and a determination of needs. This assessment includes identifying cost-effective policies and related controls. The policies and controls, as well as the risks that prompted their adoption, must be communicated to those responsible for complying with them and implemented. Finally, and perhaps most important, there must be procedures for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action. In addition, our study found that a strong central security management focal point can help

[11]Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

ensure that the major elements of the risk management cycle are carried out and can serve as a communications link among organizational units.

Since our April 1997 report, IRS has taken several actions consistent with the risk management cycle described above to improve its servicewide computer security management program. For example, IRS created the Office of Systems Standards and Evaluation as the central focal point for computer security within IRS, published revised computer security policies and procedures, promoted security awareness, and is evaluating controls at many of its facilities. However, several actions have not yet been completed or performed. For example, IRS has not fully (1) assessed risks for all of its facilities, networks, major systems, and data, (2) evaluated controls over key computing resources, and (3) implemented actions to eliminate or mitigate all of the weaknesses identified during computer control evaluations. IRS is planning or taking actions to implement these elements as part of its new strategy for its servicewide computer security management program. Until IRS fully implements an effective computer security management program, IRS is exposed to the risk that other computer control weaknesses could occur and not be detected promptly enough to prevent unnecessary losses or disruptions.

Existing Weaknesses Still Pose Significant Risk to Taxpayer Data

Although IRS has mitigated many computer security weaknesses, weaknesses in IRS' computer security controls continue to place IRS' automated systems and taxpayer data at serious risk to both internal and external threats that could result in the denial of computer services or in the unauthorized disclosure, modification, or destruction of taxpayer data. Serious weaknesses still persist at all five of the facilities included in our April 1997 report and at a sixth facility reviewed in conjunction with this audit. Our current review identified weaknesses that remain uncorrected at the five facilities visited during our prior audit and additional weaknesses we identified at those locations and at a sixth facility included in this review. The weaknesses primarily pertained to the following six functional areas: physical security, logical security, data communications, risk analysis, quality assurance, and contingency planning. These weaknesses expose taxpayers to an increased risk of loss and damages due to identity theft and other financial crimes resulting from the unauthorized disclosure and use of information they provide to IRS. A synopsis of these weaknesses by functional area follows.

Physical Security

Physical security involves restricting physical access to computer resources, usually by limiting access to the buildings and rooms where these resources are housed to protect them from intentional or unintentional loss or impairment. Physical access control measures such as locks, guards, fences, and surveillance equipment are critical to safeguarding taxpayer data and computer operations from internal and external threats. We found continuing and new physical security weaknesses at the facilities visited. The following are examples of weaknesses that have not yet been corrected.

- Access to sensitive computing areas, such as computer rooms, data communications areas, and tape libraries was not adequately controlled. For example, non-librarians without a legitimate business need could gain unauthorized access to sensitive tape libraries because there were no additional control measures restricting access to tape libraries from other controlled areas.
- Facilities visited could not account for a total of 397 missing computer tapes, some of which contain sensitive taxpayer data or privacy information.

Logical Security

Logical security controls are designed to limit or detect access to computer programs, data, and other computing resources to protect these resources from unauthorized modification, loss, and disclosure. Logical security control measures include the use of safeguards incorporated in computer hardware, system and application software, communication hardware and software, and related devices. These safeguards include user identification codes, passwords, access control lists, and security software programs. Logical controls restrict the access of legitimate users to the specific systems, programs, and files they need to conduct their work and prevent unauthorized users from gaining access to computing resources. Controls over access to and modification of system software are essential to protect the overall integrity and reliability of information systems.

We identified weaknesses relating to logical security controls at the six sites reviewed. Examples of uncorrected vulnerabilities include the following.

- Computer support personnel whose job responsibilities did not require it were given the ability to change, alter, or delete taxpayer data and associated programs.

- Access to system software was not limited to individuals with a need to know. For example, we found that database administrators[12] had access to system software, although their job functions and responsibilities did not require it.
- The powerful "root" authority, which allows users to read, modify, and delete any data file, execute any program, and activate or deactivate audit logs, had been granted to 12 computer systems analysts at one facility whose assigned duties did not require such capabilities.
- Individuals without a need to know had access to key system logs that provided the capability to perform unauthorized system activities and then alter the audit trail to avoid detection.
- Tapes and disks containing taxpayer data were not overwritten prior to reuse, thus potentially allowing unauthorized access to sensitive data and computer programs.
- Security software was not configured to provide optimum security over tape media.

In addition, IRS' ability to detect and monitor unauthorized access by employees remains limited. The information system, Electronic Audit Research Log, developed by IRS to monitor and detect browsing can not detect all instances of browsing or unauthorized access to taxpayer records because it only monitors employees using the Integrated Data Retrieval System, the primary computer system IRS employees use to access and adjust taxpayer accounts. The Electronic Audit Research Log does not monitor the activities of IRS employees using other systems, such as the Distributed Input System and Totally Integrated Examination System, which are also used to create, access, or modify taxpayer data. In addition, the Electronic Audit Research Log does not adequately distinguish potential unauthorized accesses to taxpayer data from legitimate activity. As a result, the effort to investigate potential unauthorized accesses is time-consuming and difficult. IRS is developing a new system, the Audit Trail Lead Analysis System, which is intended to improve its capability to distinguish between unauthorized accesses and legitimate activity. If properly implemented, this system would improve IRS' capability to detect unauthorized accesses to taxpayer data. However, the Audit Trail Lead Analysis System is not scheduled to be implemented until January 1999 and will only monitor the activities of IRS employees using the Integrated Data Retrieval System and not other systems used to create, access, or modify taxpayer data.

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

As a result of these logical security weaknesses, taxpayer and other sensitive data and programs were placed at unnecessary risk of unauthorized modification, loss, and disclosure without detection.

Data Communications

Data communications management is the function of monitoring and controlling communications networks to ensure that they operate as intended and securely transmit timely, accurate, and reliable data. Without adequate data communications security, the data being transmitted can be destroyed, altered, or diverted, and the equipment itself can be damaged. We identified data communications weaknesses at IRS facilities. Examples of the weaknesses existing at the time of our review include the following.

- Telecommunications equipment was still not physically protected, thus increasing the risk of improper use, modification, or destruction of data, as well as potential equipment damage. For example, telecommunications patch panels were not placed in a locked closet or enclosure, thereby increasing the risk of unauthorized tampering with these telecommunication connections.
- Dial-in access was not adequately protected. For example, data transmitted over telecommunications lines were not encrypted. Because plain text was transmitted, sensitive taxpayer data remained vulnerable to unauthorized access and disclosure.

Risk Analysis

The purpose of a risk analysis is to identify security threats, determine their magnitude, and identify areas needing additional safeguards. Without these analyses, systems' vulnerabilities may not be identified and appropriate controls may not be implemented to correct them. We found weaknesses in this area at the facilities visited. For example, we found that risk analyses of the facilities' local networks had not been performed or were not available. Without these analyses, IRS system vulnerabilities may go undetected, thereby jeopardizing IRS processing operations and sensitive taxpayer data.

Quality Assurance

Controls over the design, development, and modification of computer software help to ensure that all programs and program modifications are properly authorized, tested, and approved. An effective quality assurance program requires reviewing software products and software change control activities to ensure that they comply with the applicable processes, standards, and procedures and satisfy the control and security

requirements of the organization. One aspect of a quality assurance program is validating that software changes are adequately tested and will not introduce vulnerabilities into the system. We identified weaknesses at IRS facilities. Examples of these weaknesses follow.

- There was no independent quality assurance review or testing of locally developed programs.
- Application programmers have the capability to access or modify production computer software programs after the programs have been reviewed or tested, increasing the risk of unauthorized changes to production programs.
- Application programmers use real taxpayer data for software testing purposes, increasing the risk that sensitive taxpayer data could be disclosed to unauthorized individuals.

Without adequate quality assurance and control over the software development and change process, IRS runs a greater risk that software supporting its operations will not (1) produce reliable data, (2) execute transactions in accordance with applicable laws, regulations, and management policies, or (3) effectively meet operational needs.

Contingency Planning

An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. For this reason, organizations should have (1) established procedures for protecting information resources and minimizing the risk of unplanned interruptions, (2) a disaster recovery plan for restoring critical data processing capabilities, and (3) a business resumption plan for resuming business operations should interruptions occur.

Disaster recovery and business resumption plans specify emergency response procedures, backup operations, and postdisaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency. These plans address how an organization will deal with a full range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plans also identify essential business functions and rank resources in order of criticality. To be most effective, disaster recovery and business resumption plans should be periodically tested and employees should be trained in and familiar with the use of these plans.

We found weaknesses relating to contingency planning at the facilities reviewed, as the following examples illustrate.

- Disaster recovery plans had not been completed or lacked essential information, such as designation of an alternate computer processing site, telecommunications requirements, and procedures for restoring mission-critical processes and applications.
- Disaster recovery procedures were not adequately tested to determine IRS' ability to restore and operate all mission-critical applications.
- Disaster recovery goals and milestones were not developed based on users' business needs, which provides little assurance that users' processing needs will be met in the event of a disaster.
- Business resumption plans had not been developed or were incomplete.
- Backup generator capacity or the alternate electrical power source did not effectively meet the needs of the facilities.

Due to the nature of these and other weaknesses, IRS facilities may not be able to recover their data processing capabilities, resume business operations, and restore critical data promptly in the event of a disaster or disruption of service. Consequently, IRS has little assurance that during a crisis (1) the cost of recovery efforts or the reestablishment of operations at a remote location will be kept to a minimum, (2) taxpayer data will not be lost, (3) transactions will be processed accurately and correctly, and (4) complete and accurate taxpayer, financial, or management information will be readily available.

Conclusions

IRS has made significant progress in correcting its serious weaknesses in computer security controls intended to safeguard IRS computer systems, data, and facilities. However, serious weaknesses remain uncorrected and IRS has not yet fully assessed all of the risks to its computer processing operations nor has it evaluated the effectiveness of computer controls over key computing resources, which indicates that the service does not know the full extent of its computer security vulnerabilities. Until IRS identifies and corrects all of its critical computer security weaknesses and fully institutionalizes an effective servicewide computer security management program, the service will continue to expose its tax processing operations to the risk of disruption; taxpayer data to the risk of unauthorized use, modification, and destruction; and taxpayers to loss and damages resulting from identity fraud and other financial crimes.

Recommendations

We recommend that the Commissioner of Internal Revenue direct the Chief Information Officer and Director of the Office of Systems Standards and Evaluation to work in conjunction with the facility directors as appropriate to continue efforts to

- implement appropriate control measures to limit physical access to facilities, computer rooms, and computing resources based on job responsibility;
- limit access authority to only those computer programs and data needed to perform job responsibilities and review access authority regularly to identify and correct inappropriate access;
- configure security software to provide optimum security over tape media;
- establish adequate safeguards over telecommunications equipment and remote access to IRS systems;
- ensure that all computer programs and program modifications are authorized, tested, and independently reviewed and that real taxpayer data is not used for software testing; and
- establish controls that ensure that disaster recovery plans and business resumption plans are comprehensive, current, and fully tested.

We also recommend that the Commissioner of Internal Revenue ensure that IRS completes the implementation of an effective servicewide computer security management program. This program should include procedures for

- assessing risks for all of IRS' facilities, networks, major systems, and taxpayer data on a regular, ongoing basis to ensure that controls are adequate;
- periodically evaluating the effectiveness of controls over key computing resources at IRS facilities; and
- implementing actions to correct or mitigate weaknesses identified during such computer control evaluations.

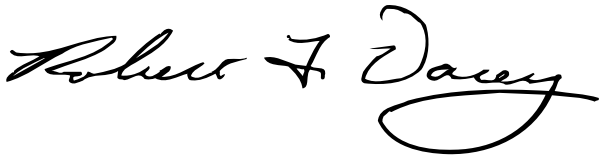
Agency Comments and Our Evaluation

In commenting on a draft of this report, IRS agreed with our recommendations and stated that the report's conclusions and recommendations are consistent with its ongoing actions to improve systems security. IRS specified the actions it has taken or plans to take to adequately mitigate the remaining weaknesses and stated that an additional 12 percent of the weaknesses have been corrected since the completion of our review. We will review the actions taken by IRS to

mitigate the remaining weaknesses as part of our audit of IRS' fiscal year 1998 financial statements.

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

If you have questions about this report, please contact me at (202) 512-3317. Major contributors to this report are listed in appendix II.



Robert F. Dacey
Director, Consolidated Audits and
Computer Security Issues

Comments From the Internal Revenue Service

COMMISSIONER

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

November 6, 1998

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

Dear Mr. Dodaro:

Thank you for the opportunity to comment on your draft report (i.e., B-280810) on systems security at the Internal Revenue Service (IRS). In general, it provides a factual cataloging and status of weaknesses found by the General Accounting Office (GAO) at five IRS facilities earlier this year. It also provides conclusions and recommendations, which are consistent with our ongoing actions to improve systems security. In this regard, we agree with your recommendations.

The draft report notes that the IRS corrected 63 percent of the weaknesses, which were originally identified in a 1997 GAO report. Since your review, an additional 12 percent of the weaknesses have been corrected. In 1997, the IRS' Office of Systems Standards and Evaluation (SSE) became the Service's central focal point to improve the management of the IRS' security. Two executives, who have years of GAO experience in systems and security reviews, were selected to manage the IRS' security program. They report directly to the IRS' new Chief Information Officer, Paul J. Cosgrave, who like myself brings years of private-sector systems and security expertise to the IRS.

The centralized executive-level leadership provided by SSE is consistent with the Risk Management Cycle model that was identified in your draft report. In this regard, SSE's efforts are continually moving through the cycle by (1) assessing risks and determining needs at facilities; (2) working with the management of the facilities and support functions to implement policies and controls, which include action plans for prioritizing and obtaining resources for corrective actions; (3) developing and implementing aggressive awareness and training programs; (4) performing follow-up announced and unannounced reviews of these facilities to monitor and evaluate success, and to reassess risks and needs.

We believe that managing risk and prioritizing corrective actions and resources is the key to making needed and measurable improvements. SSE's initial efforts were focused on the serious weaknesses at IRS' larger data processing facilities, which are critical in processing and safeguarding taxpayer data. These are the same facilities that

the GAO has focused its review efforts. By December 1998, SSE also plans to complete initial assessments of all the IRS' district offices. It will start assessing other facilities in 1999.

Hopefully, you will agree that the IRS' timely and measurable progress in this area reflects a commitment to a strong security program. We believe that actions being taken to improve security and to adequately address the remaining weaknesses reinforce this commitment. Because the report provides no opinion on these actions--which were included in the IRS' responses to each weakness—we plan to continue our ongoing efforts to adequately mitigate the remaining weaknesses.

An important benefit derived from the IRS' security program is that the Service has started to manage its risks and focus its resources on mitigating serious weaknesses. In this regard, the weaknesses identified in your report are not all serious, so some of the planned corrective actions may not be as important to quickly implement as others. It also should be noted that assessing and mitigating risks at our over 1,000 facilities cannot be completed in a few years. It is a progressive and continuous process, requiring the commitment and involvement of SSE and many other IRS offices. As in any entity, the resources available for security enhancements and upgrades will continue to be prioritized to deal with high-risk areas, where the more serious weaknesses emerge. By managing risk, however, a strong security program can provide the necessary safeguards.

In closing, thank you for helping us to assess the IRS' systems security. Protecting taxpayer information and the systems used to deliver services to taxpayers are key to the success of a customer-focused IRS. We look forward to your continuing support on this issue.

Sincerely,

Charles O. Rossotti

Major Contributors to This Report

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

Gregory C. Wilshusen, Assistant Director, (202) 512-6244
Ronald E. Parker, Senior Information Systems Analyst
Walter P. Opaska, Senior Information Systems Auditor

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 37050
Washington, DC 20013

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 (202) 512-6061, or TDD (202) 512-2537.

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