United States General Accounting Office

GAO

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

February 2001

INFORMATION SECURITY

IRS Electronic Filing Systems

GAO-01-306

GAO
Accountability * Integrity * Reliability

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

February 16, 2001

The Honorable Fred Thompson
Chairman, Committee on Governmental Affairs
United States Senate

Dear Mr. Chairman:

In connection with your request that we evaluate the effectiveness of the Internal Revenue Service's (IRS) computer controls over its external access points and internal networks and systems, we assessed the effectiveness of key computer controls designed to ensure the security, privacy, and reliability of IRS' electronic filing systems and electronically filed taxpayer data during last year's tax filing season. This report discusses computer control weaknesses that existed in IRS' electronic filing systems during the 2000 tax filing season and describes actions IRS has taken to correct these weaknesses prior to the current 2001 tax filing season.[1]

IRS maintains and operates several computerized information systems to support its electronic filing (*e-file*) program. These electronic filing systems receive tax returns telephonically from taxpayers or electronically from IRS trading partners,[2] acknowledge the receipt of information, perform editing and data validation routines on tax return data received, format the information for mainframe processing, and pass "perfected" information on to the master files.[3]

Electronic filing of income tax returns offers benefits to both taxpayers and IRS. IRS reports that taxpayers receive refunds faster and believes that electronic filing improves accuracy, decreases processing costs, and ensures the security and privacy of taxpayer data.

[1]We also plan to issue a "Limited Official Use" version of this report that provides a more detailed discussion of the computer control weaknesses and IRS' corrective actions described herein.

[2]IRS trading partners are commercial firms and individuals that IRS has authorized to participate in the electronic filing program. These partners include electronic return originators, who prepare electronic returns for taxpayers, and transmitters, who transmit the electronic portion of a return directly to IRS.

[3]Master files are the large central databases that contain historical and current detailed information on taxpayers' personal data, filing status, tax returns, and return-related documents.

IRS plans to significantly expand its electronic filing initiative. The IRS Restructuring and Reform Act of 1998 established a goal for IRS that 80 percent of all tax and information returns be filed electronically by 2007. Further, the President's fiscal year 2001 budget request specified that IRS offer, no later than tax year 2002, one or more options to the public for preparing and filing individual income tax returns over the Internet at no cost to the taxpayer.

Results in Brief

During last year's 2000 tax filing season, IRS did not implement adequate computer controls to ensure the security of its electronic filing systems and electronically transmitted taxpayer data. According to IRS officials, they have corrected most of the access control weaknesses we identified, including correction of the critical weaknesses, prior to the current 2001 tax filing season. We will assess the effectiveness of IRS' corrective actions as part of our normal follow-up review.

During the 2000 tax filing season, IRS did not adequately secure access to its electronic filing systems or to the electronically transmitted tax return data those systems contained. We demonstrated that unauthorized individuals, both internal and external to IRS, could have gained access to IRS' electronic filing systems and viewed and modified taxpayer data contained in those systems during the 2000 tax filing season. We were able to gain such access because IRS at that time had not (1) effectively restricted external access to computers supporting the *e-file* program, (2) securely configured the operating systems of its electronic filing systems, (3) implemented adequate password management and user account practices, (4) sufficiently restricted access to computer files and directories containing tax return and other system data, or (5) used encryption to protect tax return data on *e-file* systems. Further, these weaknesses jeopardized the security of sensitive business, financial, and taxpayer data on other critical IRS systems that were connected to *e-file* computers through its servicewide network. While IRS stated it did not have evidence that such intrusions occurred or that intruders accessed or modified taxpayer data on its *e-file* systems, the agency at that time did not have adequate procedures to detect such intrusions. These serious access control weaknesses existed because IRS had not taken adequate steps to assess security risks and monitor the effectiveness of security controls over taxpayer data in its e-file systems on an ongoing basis.

IRS moved promptly to correct the access control weaknesses we identified prior to the current 2001 tax filing season. IRS developed

corrective action plans to improve security over its electronic filing systems and internal networks and said it has substantially implemented those plans. As part of our normal follow-up on recommendations we make, we will test the effectiveness of these actions. Sustaining effective computer controls in today's dynamic computing environment will require top management attention and support, disciplined processes, and continuing vigilance.

Application controls also need to be designed and implemented to ensure the reliability of data processed by the systems. IRS believes that electronically filed tax returns are more accurate than paper returns and has implemented many application controls designed to enhance the reliability of data processed by its electronic filing systems. However, we identified additional opportunities to strengthen application controls for IRS' processing of electronic tax return data. Based on agency statistics, IRS processed electronic tax returns and paid refunds of about $2.1 billion without receiving required authenticating signatures from taxpayers. Edit and data validation routines on an electronic filing system did not detect certain erroneous or invalid data. In addition, weaknesses in software development controls increased the risk that individuals could have made unauthorized changes to software programs during the 2000 tax filing season.

Further, taxpayers who electronically filed may not have been aware that transmitters could have viewed and modified taxpayers' electronic tax return data and that such data are transmitted to IRS in clear text; that is, in human readable form. Transmitters possessed tax return data in clear text because IRS required most electronic filers to use the services of a transmitter and decided not to accept electronic tax returns in encrypted form.

We have made technical recommendations to improve specific access controls over IRS electronic filing systems and networks. We have also recommended that IRS complete the certification and accreditation of its electronic filing systems, assess security risks and routinely monitor the effectiveness of access controls over electronic filing systems, improve certain data reliability and integrity controls, and notify electronic filers of the privacy risks of filing electronically. Ensuring that corrective actions are effective on a continuing basis and that new risks are promptly identified and addressed will continue to be important to the way IRS plans and manages its information security program for the electronic filing program.

In commenting on this report, the IRS Commissioner generally concurred with our findings and recommendations. The Commissioner stated that IRS has completed corrective actions for all of the critical access control vulnerabilities we identified and, as a result, the electronic filing systems now satisfactorily meet critical federal information security requirements to provide strong controls to protect the taxpayer. The Commissioner also provided other comments relating to our report, which we address in appendix II.

Background

Information security is an important consideration for any organization that depends on information systems and computer networks to carry out its mission or business. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. However, without proper safeguards, these developments pose enormous risks that make it easier for individuals and groups with malicious intent to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer networks and systems. Further, the number of individuals with computer skills is increasing, and intrusion, or hacking, techniques are readily available and relatively easy to use. The rash of cyber attacks launched in February 2000 against major U.S. firms illustrates the risks associated with this new electronic age.

Computer-supported federal operations are also at risk. Our previous reports, and those of agency inspectors general, describe persistent computer security weaknesses that place a variety of critical federal operations, including those at IRS, at risk of disruption, fraud, and inappropriate disclosure.[4] This body of audit evidence led us, in 1997 and again in 1999 reports to the Congress,[5] to designate computer security as a governmentwide high-risk area. It remains so today.[6]

[4]*Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000).

[5]*High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1997) and *High-Risk Series: An Update* (GAO/HR-99-1, January 1999).

[6]*High-Risk Series: An Update* (GAO-01-263, January 2001).

How well federal agencies are addressing these risks is a topic of increasing interest in both the Congress and the executive branch. This is evidenced by recent hearings on information security,[7] recent legislation intended to strengthen information security,[8] and the President's January 2000 *National Plan for Information Systems Protection*.[9] As outlined in this plan, a number of new, centrally managed entities have been established and projects initiated to assist agencies in strengthening their security programs and improving federal intrusion-detection capabilities.

IRS Is a Major Steward of Personal Taxpayer Information

In its role as the nation's tax collector, IRS has a demanding responsibility in collecting taxes, processing tax returns, and enforcing the nation's tax laws. IRS processes more than 150 million tax returns, accounts for approximately $1.9 trillion in collections, and pays about $185 billion in refunds to taxpayers annually. To efficiently fulfill its tax processing responsibilities, IRS places extensive reliance on interconnected computer systems to perform various functions, such as collecting and storing taxpayer data, processing tax returns, calculating interest and penalties, generating refunds, and providing customer service.

Due to the nature of its mission, IRS collects and maintains a significant amount of personal and financial data on each American taxpayer. These data typically include the taxpayer's name, address, social security number, dependents, income, source of certain types of income, and certain deductions and expenses. The confidentiality of this sensitive information is important because American taxpayers could be exposed to a loss of privacy and to financial loss and damages resulting from identity theft and financial crimes should this information be disclosed to unauthorized individuals.

[7] *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000) and *Computer Security: Critical Federal Operations and Assets Remain at Risk* (GAO/T-AIMD-00-314, September 11, 2000).

[8] Government information security provisions in Fiscal Year 2001 Defense Authorization Act (Public Law 106-398, Division A, Title X, Subtitle G, Section 1061, October 30, 2000).

[9] *Defending America's Cyberspace: National Plan for Information Systems Protection: An Invitation to a Dialogue*, issued by the President on January 7, 2000.

E-File Is a Major IRS Tax Filing Initiative

IRS' *e-file* program offers taxpayers an alternative to filing traditional paper returns. With *e-file*, a taxpayer may file an electronic tax return (1) through a tax professional who is also an authorized IRS *e-file* provider, (2) through a personal computer to an *e-file* transmitter, or (3) over the telephone. The *e-file* program is beneficial because IRS receives tax and information returns in electronic form and does not have to manually enter data into its computer systems as it does with paper returns. IRS has asserted that data on electronic tax returns cost less to process and are more accurate than on paper returns, taxpayers receive refunds faster, and taxpayer privacy and security are assured.

The number of individuals filing returns electronically is increasing. During 2000, IRS reported that over 35 million individual taxpayers, about 20 percent more than the previous year, filed their returns electronically. The number of e-file individual returns represented about 28 percent of all individual returns projected to be filed during 2000. The IRS Restructuring and Reform Act of 1998 established a goal that 80 percent of all tax and information returns be filed electronically by 2007.

In an attempt to meet this goal, IRS has aggressively marketed the *e-file* program and has authorized private firms and individuals to be its *e-file* trading partners. These partners include electronic return originators, who prepare electronic tax returns for taxpayers, and transmitters, who transmit the electronic portion of a return directly to IRS. Except for taxpayers who file electronic returns using telephones, IRS does not allow individual taxpayers to transmit their electronic tax returns directly to the agency. Electronic filers must use the services of an IRS trading partner.

The Director, Electronic Tax Administration, is responsible for overseeing IRS' electronic tax programs, including *e-file*, and for improving taxpayer awareness of electronic tax administration products and services. The Chief Information Officer has overall responsibility for developing, operating, and securing IRS information systems including those used for electronic filing. The Director, Submission Processing, is responsible for processing electronically filed tax returns.

E-File Vulnerabilities Could Have Allowed Intruders to Obtain Taxpayer Data During the 2000 Tax Filing Season

Computer access controls are key to ensuring that only authorized individuals gain access to sensitive and critical agency data. They include a variety of tools, such as telecommunications and network control devices, including secure dial-in[10] and firewalls,[11] which can be used to prevent or limit inappropriate access to information system resources; passwords, intended to authenticate authorized users; and encryption, which can be used to keep the contents of a message or data file confidential if security is breached.

IRS did not adequately safeguard tax return data on *e-file* computers. Our tests, conducted in May 2000, showed that access controls over IRS' electronic filing systems were not effective in adequately reducing the risk of intrusions and misuse of electronically filed taxpayer data. We demonstrated that unauthorized individuals, both internal and external to IRS, could have viewed and modified electronically filed taxpayer data on IRS computers. For example, we were able to access a key electronic filing system using a common handheld computer.

We identified weaknesses that, if exploited during the 2000 tax filing season, could have allowed unauthorized individuals to have viewed, copied, or modified files containing electronically filed tax return data before they were sent to the IRS mainframe computer for further processing and to have viewed, altered, deleted, or redirected network traffic. In summary, during the 2000 tax filing season,

- IRS did not effectively restrict external access to its computers supporting the *e-file* program. A firewall and similar perimeter defenses are an organization's first line of defense against outside intrusion. However, IRS had not installed effective perimeter defenses to protect its *e-file* computers.
- IRS did not securely configure the operating system on its *e-file* computers. We demonstrated, for example, that the operating system

[10]Secure dial-in is a service that provides additional security over remote access from the Public Switched Telephone Network and includes the use of encryption and modem devices.

[11]A firewall is a software package and/or hardware device that controls the content of inbound and outbound computer network traffic, allowing only authorized traffic through its filters.

permitted the use of several risky and unnecessary services that could have aided an intrusion attempt.

- IRS did not implement adequate password management and user account practices on its *e-file* computers. We identified serious weaknesses in IRS' controls over the confidentiality and complexity of its passwords and in the administration of its user accounts. For example, we were able to guess many passwords based on our knowledge of commonly used passwords. We also found user-IDs and passwords that were posted in clear view on a monitor in an unsecured area at one IRS data processing facility. Poor password management and user account practices increased the risk that unauthorized individuals could determine password and user account combinations to gain unauthorized access to IRS *e-file* systems.
- IRS did not sufficiently restrict access to computer files and directories containing tax return and other system data. We determined that certain *e-file* system users with no need for access to electronically filed tax return data could have viewed and modified that data, contrary to IRS' "need to know" policy. In addition, we determined that all system users had the capability to modify numerous files on *e-file* computers, including sensitive data and system files, leaving those files much more susceptible to inadvertent or deliberate unauthorized modification.
- IRS did not encrypt tax return data while the data were stored on *e-file* computers. The *Internal Revenue Manual* requires that cryptography be used for protecting information systems from the threat of intruders gaining access by way of remote telephone systems, a threat applicable to *e-file* computers.

Intruders Could Have Accessed Other IRS Systems

IRS did not ensure the protection of sensitive business, financial, and taxpayer data on other critical systems in its servicewide network during the 2000 tax filing season. Weak controls over internal IRS networks could have allowed intruders to use *e-file* computers to gain unauthorized access to other IRS systems. Certain network control devices—largely intended to protect other internal IRS computer systems from unauthorized access—were not effectively configured or deployed to prevent such intrusions. For example, IRS personnel "turned off" (bypassed) the network control devices in order to speed up the processing of electronic tax returns. However, these actions exposed other systems attached to IRS' wide area network to unauthorized access. Along with the results of our computer control reviews at several IRS facilities, we determined that control weaknesses over other IRS networks and systems increased the risk of successful intrusions into those other systems.

IRS Procedures for Detecting Intrusions Were Inadequate

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they take steps to promptly detect intrusions and misuse before significant damage can be done. Documenting and analyzing security problems and incidents are effective ways for organizations to gain a better understanding of threats to their information and operations and of the costs of their security-related problems. Such analyses can pinpoint vulnerabilities that need to be addressed to help reduce the risk of similar intrusions and misuse.

While IRS stated that it did not have evidence that intruders accessed or modified taxpayer data on its *e-file* systems, its capabilities for detecting intrusions and misuse resulting from the exploitation of vulnerabilities on *e-file* systems during the 2000 tax filing season were not adequate. IRS did not record certain key events in system audit logs, did not regularly review those logs for unusual or suspicious events or patterns, and had not deployed software to facilitate the detection and analysis of logged events. For example, IRS did not recognize or record much of the activity associated with our test activities.

IRS Did Not Ensure Ongoing Security of *E-File* Systems

These serious access control weaknesses existed because IRS had not taken adequate steps during the 2000 tax filing season to ensure the ongoing security of electronically transmitted tax return data on its *e-file* systems. For example, IRS had not followed or fully implemented several of its own information security policies and guidelines when it developed and implemented controls over its electronic filing systems. It decided to implement and operate its *e-file* computers before completing all of the security requirements for certification and accreditation.[12] Also, IRS had not fully implemented a continuing program for assessing risk and monitoring the effectiveness of security controls over its electronic filing systems.

[12]Accreditation is the formal authorization for system operation and is usually supported by certification of the system's security safeguards including its management, operational, and technical controls. Certification is a formal review and test of a system's security safeguards to determine whether or not they meet security needs and applicable requirements.

IRS Acted to Correct *E-File* Access Control Weaknesses Prior to the 2001 Tax Filing Season

IRS' senior management moved promptly to address the access control weaknesses related to electronic filing. In meetings with senior IRS management and technical staff, we alerted IRS to significant security vulnerabilities identified by our testing that warranted immediate remediation. This interaction was productive. IRS developed corrective action plans that identified the specific actions required to improve the security over *e-file* computers and IRS internal networks.

According to IRS officials, they have completed most of the planned improvements, including correction of the critical vulnerabilities, in time for the 2001 tax filing season. IRS officials stated that they have revamped the *e-file* system architecture, installed effective perimeter defenses, improved their configuration management practices, strengthened password controls, reconfigured the operating systems of *e-file* systems, established a process to identify excessive file permissions, added intrusion-detection capability, and made certain management changes. IRS stated that its actions demonstrate that it has taken a systematic, risk-based approach to correcting these weaknesses. Such an approach is important in helping to ensure that improvement efforts are effective and appropriate. It is also important that these actions to strengthen technical controls be supported by improvements in the way IRS continually manages information security. As part of our normal follow-up review of IRS' implementation of the recommendations contained in this report, we will test the effectiveness of IRS' recent improvement actions.

Other Opportunities to Strengthen the Reliability of Electronically Filed Taxpayer Data Exist

Application controls should be designed and implemented to help ensure the reliability of data processed by the application. Such controls help make certain that transactions are valid, properly authorized, and completely and accurately processed. IRS believes that electronically filed tax returns are more accurate than paper returns for several reasons. For example, commercial software used by taxpayers to prepare electronic returns contains mathematical formulas and edit routines that can help to reduce computational errors on returns. Electronic returns also eliminate the data entry errors associated with typing paper return data into IRS' tax processing systems. In addition, IRS has implemented many application controls that were designed to enhance the reliability of data processed by *e-file* computers. However, we identified additional opportunities to strengthen application controls for IRS' processing of electronic tax return data. These opportunities are discussed below.

IRS Paid Refunds Claimed on Unauthenticated Electronic Returns

A key control relating to the authenticity and accuracy of a tax return is the taxpayer's signature and certification that the return is true, correct, and complete to the best of the taxpayer's knowledge and belief. IRS requirements state that taxpayers who file tax Form 1040 electronically must submit this signature and certification to IRS on Form 8453. Certain taxpayers participating in an IRS pilot program may use an IRS-provided personal identification number to authenticate their electronically filed return in lieu of submitting Form 8453.

IRS processed electronic tax returns and paid refunds even when it did not receive a signed Form 8453 or when a personal identification number was not used to authenticate the return. This practice is inconsistent with the IRS practice of withholding payments for refunds claimed on unsigned paper returns. Agency statistics through August 24, 2000, showed that IRS did not receive Forms 8453 for almost 1.2 million—about 3 percent—of tax returns filed electronically during the 2000 tax filing season and that about 93 percent of electronically filed returns were entitled to a refund or had no balance due. According to IRS, the average refund issued for the 1999 tax filing season for on-line filers was $2,041, and for practitioner-prepared electronic returns, $1,910. Based on these statistics, IRS paid refunds of about $2.1 billion on electronic tax returns that were not authenticated by taxpayers as of August 24, 2000. Further, according to agency criminal investigators, the absence of a signed Form 8453 may preclude perjury prosecutions against taxpayers who provide false information on electronic tax returns. Unless electronic returns are supported with a signed Form 8453 or a personal identification number before paying claimed refunds, IRS is vulnerable to paying improper refunds based on unauthenticated electronically filed tax returns.

Certain Data Validation and Editing Controls Could Be Improved

Another control activity involves identifying erroneous data at the point that it enters the application system, or at some later point in the processing cycle. This is accomplished through a process called data validation and editing. Programmed validation and edit checks are key to this process and are generally performed on transaction data entering the system (before the master files are updated) and on data resulting from processing.

We identified several instances in which an *e-file* system did not detect erroneous or invalid data in our test transactions. For example, an *e-file* system did not detect several arithmetical errors and inconsistent data or amounts between related data fields on the Form 1040 and the

attachments. As a result, there was an increased risk that IRS did not detect certain erroneous or inconsistent data on electronically filed tax returns.

Software Development Controls Could Be Improved

An essential control for ensuring the integrity of a computer application is to prevent software programmers and developers from having access to the application in the production environment. Denying such access to software programmers and developers can help to reduce the risk of unauthorized changes to production programs and data.

However, a software developer was capable of viewing and modifying taxpayer data on production *e-file* computers during the 2000 tax filing season. In addition, software development tools were installed on those computers. As a result, there was an increased risk last year that the software developer could have introduced unauthorized programs, made unauthorized changes to production programs, and viewed or modified electronically filed taxpayer data on *e-file* computers.

Taxpayers May Not Be Aware of Privacy Considerations in Filing Electronic Returns

Taxpayers who electronically file tax returns may not have been aware that transmitters could view and modify taxpayers' electronic tax return data and that such data are transmitted to IRS in clear text. Transmitters have this level of access because IRS decided (1) not to allow taxpayers to file most electronic returns directly with IRS, (2) to require taxpayers who elect to file electronically to use the services of third-party transmitter, and (3) not to accept electronic tax returns in encrypted form. Also, taxpayers may not have been aware of other risks related to electronic filing. [13]

Links provided on the IRS Web site to certain IRS trading partners emphasized the use of state-of-the-art encryption when electronic filers send tax information over the Internet to IRS trading partners, but these links did not disclose that the trading-partner-to-IRS portion of the data transfer was sent in clear text. Thus, taxpayers who prepared their electronic tax returns and sent the returns in an encrypted form to a transmitter for transmission to IRS may not have known that the transmitter could have viewed, modified, or copied their tax returns, or that their returns were transmitted to IRS in clear text. Similarly, taxpayers

[13]Our review focused on electronic filing. We did not address risk considerations related to filing paper returns.

who used the services of an electronic return originator to prepare their electronic returns may not have realized that their returns were sent to IRS in clear text or that the electronic return originator may have sent their returns to a transmitter for transmission to IRS. As a result, taxpayers may not have been fully informed as to which businesses and individuals could have viewed, modified, and copied the personal and financial data contained on their electronically filed tax returns.

IRS did not adequately inform taxpayers of other risks related to filing electronic tax returns. Although IRS noted that it did not endorse the products, services, or privacy or security policies of its electronic filing trading partners, IRS asserted in promotional materials on *e-file* that the security and privacy of tax return data filed electronically was "assured." However, the security and privacy of such data were subject, in part, to the (1) effectiveness of the transmitters' security controls over their computing environments and (2) character of the transmitters' employees who had access to the taxpayer data. IRS had no assurance about the security of transmitter systems that contained or transmitted tax return data to IRS's *e-file* systems, including whether users of such systems were properly authorized, and had only limited assurance about the character or background of the transmitters.

Other than providing guidance about protecting certain passwords, IRS did not prescribe minimum computer security requirements for transmitters and did not assess or require an independent assessment of the effectiveness of computer controls within the transmitters' operating environment. IRS monitored transmitters for compliance with the applicable revenue procedure and *e-file* program requirements. According to IRS, monitoring may have included reviewing *e-file* submissions, investigating complaints, scrutinizing advertising material, visiting offices, examining files, observing office procedures, and conducting annual suitability checks. However, IRS did not assess computer security over transmitters' computer systems as part of its monitoring efforts.

In addition, although IRS stated it performed an annual suitability check of its trading partners, including *e-file* transmitters, most were not subjected to criminal background or fingerprint checks. The Treasury Inspector General for Tax Administration reported in September 1999 that although IRS improved the 1998 suitability screening process, the overall process was not completely successful in preventing inappropriate *e-file* trading partners from participating in the *e-file* program. For example, IRS had approved individuals to be *e-file* trading partners who had unpaid tax

liabilities, filed tax returns late, filed false tax returns, or had been assessed Trust Fund Recovery penalties.[14] Importantly, however, transmitters and electronic return originators may be subject to criminal or civil penalties if they improperly disclose or misuse tax return information.

Conclusions

A number of serious control weaknesses in IRS' electronic filing systems placed personal taxpayer data in IRS' electronic filing systems at significant risk of unauthorized disclosure, use, and modification during last year's tax filing season. IRS recognized the importance of promptly addressing these weaknesses and stated that it has taken steps to correct them prior to the current tax filing season. Ensuring that ongoing controls over electronic filing are effective requires top-management support and leadership, disciplined processes, and consistent oversight. IRS' efforts to achieve the goal that 80 percent of all tax and information returns be filed electronically by 2007 must be balanced with the need to adequately ensure the security, privacy, and reliability of taxpayer and other sensitive information. Failure to maintain adequate security over IRS' electronic filing systems could erode public confidence in electronically filing tax returns, jeopardize IRS' ability to meet the 80 percent goal, and deprive IRS of the many benefits that electronic filing offers.

Recommendations for Executive Action

The following recommendations are based on information security weaknesses identified during last year's 2000 tax filing season. As noted in this report, IRS has acted to correct critical weaknesses prior to the 2001 tax filing season. We will assess the effectiveness of these corrective actions as part of our normal follow-up review.

We recommend that the IRS Commissioner direct the Chief Information Officer to complete efforts to implement an action plan for strengthening access controls over IRS electronic filing systems and networks. To assist in this effort, we have provided technical recommendations that addressed specific access control weaknesses that IRS should address as part of its efforts. Because of the significance of the electronic filing systems to the future operations of IRS, we also recommend that the Chief Information

[14]Trust Fund Recovery penalties can be assessed against an individual, such as an officer of a corporation, found willful and responsible for not forwarding to the government payroll taxes withheld from their employees' salaries.

Officer periodically report to the Commissioner on progress made to implement this action plan and on the results of efforts to continually monitor the risks and effectiveness of security controls over IRS electronic filing systems and electronically filed taxpayer data.

We also recommend that the IRS Commissioner direct the Chief Information Officer to

- complete actions required for the certification and accreditation of an *e-file* system;
- fully implement procedures to assess risks and monitor the effectiveness of security controls over IRS' electronic filing systems on an ongoing basis;
- enhance the edit and data validation routines in an *e-file* system to detect erroneous or invalid data on electronically filed tax returns; and
- improve the integrity of the *e-file* production environment by
  - removing software development tools from the production environment, if feasible, or restricting access to the tools to the minimum number of users who require it and
  - disallowing developers access to production environments and taxpayer data.

We recommend that the Commissioner direct the Director of Submission Processing to implement an alternative means for taxpayers to authenticate electronically filed returns or to strengthen procedures for receiving signed Forms 8453 for electronically filed tax returns.

We recommend that the Commissioner direct the Director of Electronic Tax Administration to provide notice to taxpayers concerning (1) transmitter access to electronic tax return data in clear text and (2) electronic transmission of tax returns to IRS in clear text.

Agency Comments and Our Evaluation

In commenting on a draft of this report, the Commissioner of Internal Revenue stated that the report accurately identified areas that needed strengthening during last year's filing season and that IRS initiated timely actions to strengthen important security controls when the audit findings were brought to its attention. He further indicated that IRS has completed actions for correcting all of the critical access control vulnerabilities we identified and for certifying the systems. As a result, the Commissioner stated, the electronic filing systems now satisfactorily meet critical federal information security requirements to provide strong controls to protect

taxpayer data and that taxpayers can feel safe and secure using *e-file* during the 2001 filing season. The Commissioner added that the report's findings and GAO's assistance have been instrumental in supporting IRS' continuing efforts to improve its computer security capabilities.

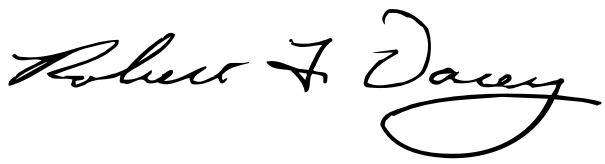
The Commissioner's written response indicated that it has taken or will take appropriate steps to implement eight of our nine recommendations. IRS' Director of Security Evaluation and Oversight stated orally that IRS has taken corrective action to resolve the final recommendation. We will assess the effectiveness of IRS' corrective actions as part of our normal follow-up review on recommendations.

In addition to responding to our recommendations, the IRS Commissioner provided additional comments about IRS' security program, our report, and other controls over electronic filing. We addressed these comments in appendix II.

As agreed with your office, unless you publicly announce the contents of this report earlier, we will not distribute it until 30 days from the date of this letter. At that time, we will send copies to Senator Joseph Lieberman and other interested congressional committees. We will also send copies of this report to the Honorable Paul H. O'Neill, Secretary of the Treasury; the Honorable Charles O. Rossotti, Commissioner of Internal Revenue; and the Honorable Mitchell E. Daniels, Jr., 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 or by e-mail at *DaceyR@gao.gov*. Key contributors to this assignment were West Coile, Hal Lewis, Karlin Richardson, and Gregory Wilshusen, (202) 512-6244, *WilshusenG@gao.gov*.

Sincerely yours,



Robert F. Dacey
Director, Information Security Issues

Objectives, Scope, and Methodology

Our objective was to assess the effectiveness of key computer controls that were designed to ensure the security, privacy, and reliability of IRS' electronic filing systems and electronically filed taxpayer data. To accomplish our objective, we applied appropriate sections of our *Federal Information System Controls Audit Manual* (GAO/AIMD-12.19.6), which describes our methodology for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized data.

To assess the security over IRS' electronic filing systems and privacy of electronically filed taxpayer data, we tested the effectiveness of key computer access controls over electronic filing systems, reviewed IRS policies and procedures, researched prior reports by IRS' Internal Audit and the Treasury Inspector General for Tax Administration, interviewed system administrators and program officials, assessed the design and architecture of *e-file* systems, and examined the operating system configuration and control implementation for electronic filing systems' host computers and network servers, routers, and control devices. In addition, we attempted to exploit identified control weaknesses to verify the vulnerabilities they presented. We also met with officials at IRS national offices to discuss the possible reasons for the vulnerabilities we identified and their plans for future improvement.

To assess the reliability of electronically filed tax return data processed by *e-file* systems, we examined controls designed to ensure that electronically filed tax return data were valid, properly authorized, and accurately and completely processed. In addition, we reviewed IRS policy and procedures; examined application system documentation; interviewed system and security administrators, users, and officials at selected IRS facilities; observed procedures and controls in place; examined transaction source documents and control documents; processed test transactions and assessed results; and inspected application logs and reports. We also assessed IRS' information system general controls and their impact on these applications.

We performed our review at several IRS facilities and at our headquarters in Washington, D.C., at various times from July 1999 through August 2000, in accordance with generally accepted government auditing standards and our *Federal Information System Controls Audit Manual*.

Comments From the Internal Revenue Service

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

COMMISSIONER

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

February 8, 2001

The Honorable David M. Walker
Comptroller General of the United States
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Walker:

Thank you for the opportunity to comment on your draft General Accounting Office (GAO) report, entitled Information Security: IRS Electronic Filing Systems, (GAO-01-306). In general, it accurately identified areas that needed strengthening when the GAO performed its audit during last year's filing season. I can assure you that the IRS takes its security and privacy responsibilities seriously. As acknowledged in your report, the IRS initiated timely actions to strengthen important security controls when your audit findings were brought to our attention. This included completing action for all the critical access control vulnerabilities identified and the systems' certification. As a result, the electronic filing systems now satisfactorily meet critical federal information security requirements to provide strong controls to protect taxpayer data.

To put it simply, taxpayers can feel safe and secure using e-filing during the 2001 filing season. We have strengthened our systems' security, and we will remain vigilant to keep our e-filing process the safest possible.

The report's findings and your staff's assistance have been instrumental in supporting the IRS' continuing efforts to improve its computer security capabilities. In addition, following are four critical issues that need to be addressed.

See comment 1.

1. As the GAO has previously noted, the IRS does have an aggressive and effective security program. This program—along with our privacy program—is actively focused on safeguarding the confidentiality of taxpayer records. Many corrective actions have been implemented to improve our computer security infrastructure since 1997, and a strong emphasis is being placed on designing security safeguards into new systems.

   Over the last 10 months, the IRS has further enhanced its security program by focusing on mission assurance, risk management, and measurable corrective actions. The program continues to improve the Service's security infrastructure, approaches and processes—while overseeing and managing risks. Of special note, the IRS has been focused on enhancing its computer security incident reporting and analysis capability for the last few years to better detect system and network intrusions. In this regard, the IRS is continuing to shift considerable resources to support its security program approach. Many planned and needed improvements are highly dependent on continuing our systems modernization efforts and on

obtaining additional funding to adequately mitigate the risks and weaknesses associated with our existing old systems infrastructure. These weaknesses are consistent with many of those that continue to be reported by GAO and the Treasury Inspector General for Tax Administration (TIGTA).

See comment 2.

2. The report does not differentiate between the likelihood of the threats occurring and the risks associated with the threats—resulting in the message unreasonably promoting undue concern. It is important to distinguish between weaknesses and areas where improvements can be made—especially, given the limited resources that need to be prioritized to adequately defend against likely threats. For example, the report implies that data sent unencrypted across the trusted U.S. public switch network is being exposed to unacceptable and increased risks. Strong laws and controls were established to protect the transmission of private information across this network. Everyday, voice calls are utilized by the public to communicate shared secrets with individuals and entities, such as credit card companies and Federal agencies. The U.S. Postal Service is another example of a trusted carrier of information. National security information is allowed to be sent by mail and by approved package delivery firms (e.g., FedEx and UPS) if it is double enveloped and addressed properly—even though their employees can be considered a threat to the confidentiality of the information. In this regard, it is important to understand that the threat is not likely given the controls established. If this has changed, then we have a much bigger national problem.

See comment 3.

We do agree that providing an encryption option to transmitters will help to strengthen existing controls. In this regard, we are assessing the feasibility and cost-benefit of encrypting electronic tax return information during transmission.

See comment 4.

3. It should be stated that there was no evidence of anyone compromising the systems reviewed. This is especially important given that there are other inherent controls that exist. For example, taxpayers and their preparers provide controls that protect their interests because they would have notified the IRS if their reported tax liabilities were changed.

4. The IRS will notify taxpayers on its website that they need to be aware that there are inherent risks associated with using third parties to prepare and file tax returns. It should be noted that transmitters, along with Electronic Return Originators (ERO), are considered trusted partners. As such, if tax return information is misused, the transmitter may be subject to criminal penalties under §301.7216-1(a), or civil penalties under §6713 for unauthorized disclosure or use of tax return information. Additionally, they undergo an annual suitability check, which includes a review of tax returns filed, and tax liabilities. The TIGTA report referred to applications/cases randomly selected in 1997 to verify accuracy of suitability determinations. The One Site Application and Suitability process was established later that year for the very purpose of insuring that consistent and stringent procedures would be used to screen applicants.

See comment 5.

See comment 6.

Additionally, the IRS monitors authorized e-file providers for compliance with the revenue procedure and program requirements. Monitoring may include reviewing IRS e-file submissions, investigating complaints, scrutinizing advertising material, checking Form 8453 submissions, visiting offices, examining files, observing office procedures and conducting annual suitability checks. Violations may result in warnings or in sanctioning of the authorized e-file provider. Sanctioning may be a written reprimand, suspension or expulsion from the program or other sanctions depending on the seriousness of the infraction. Because EROs and transmitters have access to taxpayer data, stringent suitability requirements are monitored and enforced for the duration of their participation in the e-file program. In processing year 2000, 224 new applications to participate in the program have been rejected and 703 program participants have been suspended based on these screenings. Because of these controls, we believe the risk of taxpayer data coming through transmitters is no greater than that of the risk of taxpayer data coming through the mail in paper format.

Enclosed is Appendix I, which addresses your recommendations. I request that this letter and its appendix be included in your final report.

Again, thank you for assisting the IRS' continuing efforts to improve its computer security capabilities. If you have any questions, or if you would like to discuss this response in more detail, please contact me, or have your staff contact Len Baptiste, who directs the IRS security program, at 202-622-8910.

Sincerely,

Charles O. Rossotti

Charles O. Rossotti

Enclosure

Internal Revenue Service Response to GAO Recommendations

Recommendations For Executive Action

We recommend that the IRS Commissioner direct the Chief Information Officer to complete efforts to implement an action plan for strengthening access controls over IRS electronic filing systems and networks. Because of the significance of the electronic filing systems to the future operations of IRS, we also recommend that the Chief Information Officer periodically report to the Commissioner on progress made to implement this action plan and on the results of efforts to monitor on a continuing basis the risks and effectiveness of security controls over IRS electronic filing systems and electronically filed taxpayer data.

IRS Response: IRS developed an action plan to address the GAO recommendations.

IRS Response: The CIO will periodically report to the Commissioner on progress made to implement the action plan. In addition, the Security Evaluation and Oversight Office will conduct independent reviews to ensure actions have been completed as prescribed by the action plan.

We also recommend that the IRS Commissioner direct the Chief Information Officer to:

- complete actions required for the certification and accreditation an e-file system,

  IRS Response: The certification and accreditation the system is complete.

- fully implement procedures to assess risks and monitor the effectiveness of security controls over IRS' electronic filing systems on an ongoing basis,

  IRS Response: Procedures have been initiated to better assess risks and monitor the effectiveness of security controls.

- Enhance the edit and data validation routines in an e-file system to detect erroneous or invalid data on electronically filed tax returns, and

  IRS Response: IRS will continue to enhance edit and validation routines to detect erroneous or invalid data on the system. There was one exception where the system was not programmed to validate that the taxpayer identification number on the return and on the attachment matched. We identified the error and were prepared to correct the situation; however, subsequently, the form was revised and the taxpayer identification information is no longer needed. Therefore, for tax year 2000, all situations where it is required, the system will validate that the taxpayer identification number on the return and on the attachment is the same.

1

Internal Revenue Service Response to GAO Recommendations

Concerning the math errors, because the system's returns are prepared using commercial tax preparation software packages that contain extensive arithmetical and consistency validations, the system program itself does not generally perform arithmetical checks. The software, however, is reviewed during testing—where the math related to tax computations is tested. In addition, mainframe processing also performs validation checks.

- Improve the integrity of the e-file production environment by disallowing developers access to production environments and taxpayer data.

  IRS Response: Developers no longer have access to the production environment and taxpayer data.

We recommend that the Commissioner direct the Director, Submission Processing to implement an alternative means for taxpayers to authenticate electronically filed returns or to strengthen procedures for receiving signed Forms 8453 for electronically filed tax returns.

IRS Response: In keeping with GAO's recommendation, a nationwide PIN program, known as the Self-Select PIN has been implemented. To authenticate the taxpayer, the taxpayer must provide to IRS his/her (1) social security number; (2) birth date; (3) AGI from the prior year tax return; and (4) total tax from the prior year return. To sign the return, taxpayers will select their own Personal Identification Number (PIN) and file electronically without any paper.

We will continue to take actions to strengthen our procedures for receiving signed Form 8453s for electronically filed returns. For example, the IRS continues to follow up with taxpayers and tax practitioners in those cases where the Form 8453s have not been received. Practitioners are suspended from the electronic filing program if the Form 8453s are not received.

We recommend that the Commissioner direct the Director, Electronic Tax Administration to provide notice to taxpayers concerning (1) transmitter access to electronic tax return data in clear text and (2) electronic transmission of tax returns to IRS in clear text.

IRS Response: The IRS will notify taxpayers on its website that they need to be aware that there are inherent risks associated with using third parties to prepare and file tax returns. We are very concerned about unreasonably alarming taxpayers on the risks associated with using the U.S. public switch network. GAO refers to a bulleted item on a now discontinued IRS web page, which noted that *"Your privacy and security are assured."* If GAO believes that this should mean total assurance, the IRS will consider never

See comment 7.

Internal Revenue Service Response to GAO Recommendations

using this statement again—especially given that total assurance is impossible. On another IRS web page that links to electronic filing transmitters, it notes that "*By linking to this private business, the IRS is not endorsing its products, services, or privacy or security policies.*"

See comment 6.

It should be noted that transmitters, along with Electronic Return Originators (EROs) are considered trusted partners. As such, if tax return information is misused the transmitter may be subject to criminal penalties under §301.7216-1(a), or civil penalties under §6713 for unauthorized disclosure or use of tax return information. Additionally, they undergo an annual suitability check, which includes a review of tax returns filed, and tax liabilities. The TIGTA report referred to applications/cases randomly selected in to verify accuracy of annual suitability determinations. These cases were worked prior to the movement of the annual suitability determinations to the One Site Application and Suitability staff at the Andover Center. The movement of the work to Andover corrected the weaknesses pointed out in the TIGTA report leading to hundreds of suspensions of program participants.

See comment 6.

Additionally, the IRS monitors authorized e-file Providers for compliance with the revenue procedure and program requirements. Monitoring may include reviewing IRS e-file submissions, investigating complaints, scrutinizing advertising material, checking Form 8453 submissions, visiting offices, examining files, observing office procedures and conducting annual suitability checks. Violations may result in warnings or in sanctioning of the authorized e-file Provider. Sanctioning may be a written reprimand, suspension or expulsion from the Program or other sanctions depending on the seriousness of the infraction.

Because EROs and Transmitters have access to Taxpayer data, stringent suitability requirements are monitored and enforced for the duration of their participation in the e-file program.

3

The following are GAO's comments on the Internal Revenue Service's letter dated February 8, 2001

GAO Comments

1. We have previously reported that although IRS has made significant strides in improving computer security at certain facilities, an effective computer security management program had not yet been fully implemented across the service.[1]

2. We agree that the report does not focus on the likelihood of the threats occurring and focuses on the risks associated with the threats. However, we do not believe the report's message unreasonably promotes undue concern about the risks associated with electronic filing. In our view, we are presenting the facts about certain risks that accompany electronic filing–risks that may or may not be present in paper filing, and risks that the public is entitled to know. Because of its role as the nation's tax collector, IRS' computer systems may be a target for certain individuals or groups. Our tests, which successfully identified and exploited weaknesses in IRS' *e-file* computers, were not sophisticated. It is important to note that IRS immediately recognized the seriousness of the weaknesses we identified and said it has taken prompt action to correct all of the critical vulnerabilities.

3. We neither state nor imply that sending data unencrypted over public switched networks is an unacceptable risk. However, we continue to believe that the risk of unauthorized disclosure is greater when electronic tax returns are transmitted in clear text than in encrypted text. It is important to note that IRS regulations require encryption and secure dial-in for remote access from the public switched telephone network to any IRS system that contains sensitive data.

4. As noted in the report, although IRS did not have evidence that intruders accessed or modified taxpayer data on its *e-file* systems, its capabilities for detecting intrusions and misuse resulting from the exploitation of vulnerabilities on *e-file* systems during the 2000 tax filing season were not adequate.

[1] *IRS Systems Security: Although Significant Improvements Made, Tax Processing Operations and Data Still at Serious Risk* (GAO/AIMD-99-38, December 14, 1998) and *Financial Audit: IRS' Fiscal Year 1999 Financial Statements* (GAO/AIMD-00-76, February 29, 2000).

5. The Treasury Inspector General for Tax Administration reported in September 1999 that although IRS improved the 1998 suitability screening process, the overall process was not completely successful in preventing inappropriate *e-file* trading partners from participating in the *e-file* program.

6. We recognize in the report that IRS performs annual suitability checks and monitors its trading partners. However, we continue to believe that taxpayers have a right to know that IRS does not subject most of its trading partners to criminal background or fingerprint checks and does not assess computer security over transmitters' computer systems as part of its monitoring efforts.

7. We do not believe that "total assurance" is necessary, only full disclosure. At the time IRS asserted on its Web page that taxpayers' "privacy and security are assured," we identified serious access control weaknesses over IRS electronic filing systems that could have allowed unauthorized individuals to view and modify taxpayer data. Further, IRS had no assurance about the effectiveness of computer controls within the transmitters' operating environments—environments that affect the privacy and security of electronically filed tax return data. We believe that IRS should inform taxpayers of the risks as well as the benefits of filing electronic tax returns so they can make informed decisions on the tax filing method that is appropriate for them.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. 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

Orders by visiting:
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
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.

Orders by Internet:
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

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- **Web site: http://www.gao.gov/fraudnet/fraudnet.htm**
- **e-mail: fraudnet@gao.gov**
- **1-800-424-5454 (automated answering system)**

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00