United States General Accounting Office

GAO

Report to the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives

May 2003

INFORMATION SECURITY

Progress Made, but Weaknesses at the Internal Revenue Service Continue to Pose Risks

GAO-03-44

May 2003

INFORMATION SECURITY

Progress Made, but Weaknesses at the Internal Revenue Service Continue to Pose Risks

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-44, a report to the Chairman and Ranking Minority Member of the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives

Why GAO Did This Study

As part of its annual audits of IRS's financial statements, GAO assessed the effectiveness of information security controls at certain IRS facilities and over certain specific applications—controls meant to protect IRS's information systems and taxpayer data. Because the detailed reports that followed these reviews contained sensitive information and could be detrimental to the government if released to the public, they were issued only to IRS and congressional requesters. This public report is based on 18 such reports issued during the 3-year period ending July 31, 2002. Although it does not identify specific IRS facilities or applications, the report does provide GAO's assessment of the overall effectiveness of IRS's information security.

What GAO Recommends

To assist IRS in implementing an effective agencywide information security program, GAO is recommending that the Commissioner of Internal Revenue direct the chief information officer and the senior management official for each operating division to assess risks and evaluate security needs, establish and implement adequate policies and controls, enhance security awareness and training, and monitor the effectiveness of controls and mitigate known weaknesses, as detailed in this report. IRS generally agreed with the report and recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-03-44.

To view the full report, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

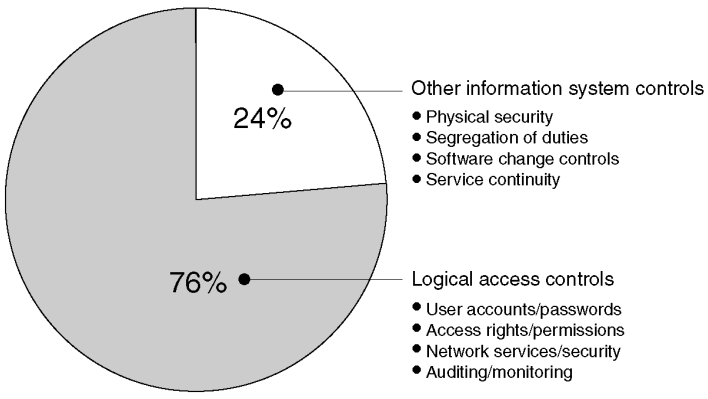
What GAO Found

IRS has made and continues to make important progress toward improving its information security and implementing a comprehensive information security program. Nonetheless, weaknesses continue to threaten the confidentiality, integrity, and availability of sensitive systems and taxpayer data. IRS's implementation of logical access controls—those designed to ensure that only authorized individuals can read, alter, or delete data—has been inconsistent and accounts for three quarters of the 765 general control weaknesses found at the 11 facilities reviewed. Weaknesses in the other four control categories (see breakdown below) have further reduced IRS's effectiveness in physically securing its assets, separating incompatible duties among individuals, preventing unauthorized changes to software programs, and ensuring the agency's ability to continue operations after an unexpected interruption. In addition, 112 application control weaknesses hindered IRS's ability to limit access to 5 key applications to authorized persons for authorized purposes. The extent of these weaknesses demonstrates that information security is an agencywide challenge.

An underlying cause of these weaknesses is that IRS had not yet fully implemented certain elements of its agencywide information security program. As a result, it had not adequately identified or assessed risks in order to determine needed security measures, implemented or complied with policies to meet those needs, promoted adequate security awareness and training, and monitored the effectiveness of policies or mitigated known security vulnerabilities.

IRS management is committed to completing such an agencywide program. Until it does, however, IRS will remain at heightened risk of access to critical data by unauthorized persons—individuals who could obtain personal taxpayer data to perpetrate identity theft and commit financial crimes.

Breakdown of Weaknesses by General Control Category



Source: GAO.

Contents

Figures

Abbreviations

CIO	Chief Information Officer
IRS	Internal Revenue Service
GISRA	Government Information Security Reform Act
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget

This is a work of the U.S. Government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. It may contain copyrighted graphics, images or other materials. Permission from the copyright holder may be necessary should you wish to reproduce copyrighted materials separately from GAO's product.

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 30, 2003

The Honorable Adam H. Putnam
Chairman
The Honorable William Lacy Clay, Jr.
Ranking Minority Member
Subcommittee on Technology, Information Policy,
Intergovernmental Relations, and the Census
Committee on Government Reform
House of Representatives

As part of our annual audits of the Internal Revenue Service's (IRS) financial statements, we assessed the effectiveness of computer-related general controls at certain IRS facilities and computer controls over certain applications.[1] For each facility or application assessed, we issued a detailed report to the IRS Chief Information Officer (CIO) that discusses facility-specific or application-specific results, conclusions, and recommendations. These reports are designated for "Limited Official Use Only" because of the sensitive nature of the information they contain and because release to the public could be detrimental to the government. During the 3-year period ending July 31, 2002, we issued 14 facility-specific reports and 4 application-specific reports.

This report summarizes our analysis of the information contained in those 18 reports and provides our assessment of the overall effectiveness of IRS's computer controls intended to protect the confidentiality, integrity, and availability of systems and taxpayer data. It also identifies key issues affecting IRS's ability to effectively implement an agencywide information security program and the status of its actions to do so. We are addressing this report to you in response to your request.

Results in Brief

IRS has made important progress toward improving information security controls and implementing an agencywide information security program. It has implemented various safeguards designed to help protect its systems from external attack and has established information security policies,

[1]General controls are the structure, policies, and procedures that apply to an organization's overall computer operations. They establish the environment in which application systems and controls operate. Application controls are the structure, policies, and procedures that apply to separate individual application systems.

standards, and guidelines that, if effectively implemented, would protect its information systems from many threats. Nonetheless, computer control weaknesses continued to threaten the confidentiality, integrity, and availability of sensitive systems and taxpayer data. IRS's inconsistent implementation of logical access controls at its facilities did not effectively prevent, limit, or detect access to computing resources. In addition, weaknesses in other information system controls (including physical security, segregation of duties, software change controls, and service continuity) reduced IRS's effectiveness in protecting and controlling physical access to assets, minimizing the risk of errors or fraud, mitigating the risk of unauthorized or inappropriate software programs, and ensuring the continuity of data processing operations when unexpected interruptions occur. Further, access to key computer applications was not always limited to authorized persons for authorized purposes. These weaknesses increased the vulnerability of data processed by IRS's information systems and continued to expose IRS's tax processing operations to disruption.

An underlying cause for these weaknesses was that, although it had made important progress, IRS had not yet fully implemented certain elements of its agencywide information security program. As a result, the agency was not adequately (1) identifying and assessing risks to determine needed security measures; (2) establishing and implementing policies and controls to meet those needs; (3) promoting awareness and providing security-related training so that employees understand the risks and the policies and controls that mitigate them; or (4) monitoring and evaluating established policies and controls, and mitigating known security vulnerabilities. IRS has acknowledged the seriousness of its information security weaknesses and has revised its approach to implementing the agencywide information security program. Until IRS can fully implement an effective program and adequately mitigate these weaknesses, it will remain at heightened risk of access to critical hardware and software by unauthorized individuals, who could intentionally or inadvertently add, alter, or delete sensitive data or computer programs. Such individuals could possibly obtain personal taxpayer information and use it to commit financial crimes in the taxpayer's name (identity fraud), such as establishing credit and incurring debt.

To assist IRS in implementing an effective agencywide information security program, we are making recommendations to the IRS Commissioner that address these issues.

In providing written comments on a draft of this report, the Commissioner of Internal Revenue generally agreed with the report, and indicated that IRS is acting to implement our recommendations.

Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where the public's trust is essential. 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. Without proper safeguards these changes 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 systems and networks.

Protecting the computer systems that support critical operations and infrastructures has never been more important because of the concern about attacks from individuals and groups with such malicious intent, including terrorists. These concerns are well founded for a number of reasons, including the dramatic increases in reported information security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks to come.

Computer-supported federal operations are likewise at risk. Our previous reports, and those of agency inspectors general, describe persistent information security weaknesses that place a variety of critical federal operations, including those at IRS, at risk of disruption, fraud, and inappropriate disclosure.[2] This body of audit evidence led us, in 1997, to

[2]U.S. General Accounting Office, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000).

designate information security as a governmentwide high-risk area in reports to the Congress.[3] It remains so today.[4]

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[5] and recent legislation intended to strengthen information security.[6] In addition, the administration undertook other important actions to improve information security, such as integrating information security into the President's Management Agenda Scorecard. Moreover, the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued security guidance to agencies.

IRS Is a Major Steward of Personal Taxpayer Information

In its role as the nation's tax collector, IRS is responsible for collecting taxes, processing tax returns, and enforcing the nation's tax laws. In fiscal year 2002, it processed about 200 million tax returns, accounted for approximately $2 trillion in collections, and paid about $281 billion in refunds to taxpayers. To efficiently fulfill its tax processing responsibilities, IRS relies extensively 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

[3]U.S. General Accounting Office, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

[4]U.S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).

[5]U.S. General Accounting Office, *Information Security: Progress Made, but Challenges Remain to Effectively Protect Federal Systems and the Nation's Critical Infrastructures*, GAO-03-564T (Washington, D.C.: Apr. 8, 2003); *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk*, GAO-03-303T (Washington, D.C.: Nov. 19, 2002); *Information Security: Comments on the Proposed Federal Information Security Management Act of 2002*, GAO-02-677T (Washington, D.C.: May 2, 2002); and *Information Security: Additional Actions Needed to Implement Reform Legislation*, GAO-02-470T (Washington, D.C.: Mar. 6, 2002).

[6]E-Government Act of 2002 (P.L. 107-347, Title III, Section 301, Dec. 17, 2002); and Government Information Security Reform Provisions in Fiscal Year 2001 Defense Authorization Act (P. L. 106-398, Division A, Title X, Subtitle G, Section 1061, Oct. 30, 2000).

data typically include the taxpayer's name, address, Social Security number, dependents, income, sources of certain types of income, and certain deductions and expenses. The confidentiality of this sensitive information is important because if this information is disclosed to unauthorized individuals, taxpayers could be exposed to a loss of privacy and to financial loss and damages resulting from identity theft and financial crimes.

To help provide information security for its operations and assets (including computing resources and taxpayer information), IRS has developed and is implementing an agencywide information security program. According to IRS, this program will, among other things, (1) ensure the confidentiality, integrity, and availability of information; (2) assign management responsibility for certifying the adequacy of security controls to protect information; (3) establish individual accountability for the data, information, and other information technology resources to which individuals have access; (4) ensure the audit capability of all information systems; and (5) provide the ability to maintain processing during and following an emergency. To accomplish these goals, IRS has developed and published information security policies, guidelines, standards, and procedures in the *Internal Revenue Manual*, *Law Enforcement Manual*, and other documents.

IRS's CIO is responsible for developing and maintaining this agencywide information security program and ensuring that (1) it provides information security for the operations and assets of the agency and (2) the agency effectively implements and maintains prescribed information security policies, procedures, and control techniques. The senior management official in each of IRS's operating divisions,[7] with the assistance of the CIO, is responsible for (1) assessing the information security risks associated with the operations and systems over which the official has control, (2) determining the levels of information security appropriate to protect such operations and systems, and (3) periodically testing and evaluating the effectiveness of information security controls and techniques. IRS's Chief of Security Services is the agency's senior agency information security official, responsible for ensuring that IRS has effective security programs

[7]IRS has reorganized itself into four major operating divisions, aligned by types of taxpayers: Wage and Investment, Small Business and Self-Employed, Large and Mid-Size Business, and Tax Exempt and Government Entities. The senior management official for each of these major divisions is a commissioner. Other operating divisions include Appeals, Chief Counsel, Communications and Liaison, and Criminal Investigation.

in place to adequately safeguard taxpayer records, employees, facilities, systems, and other resources. According to IRS, the operating budget for Security Services is about $24.5 million for fiscal year 2003.

We Have Previously Reviewed IRS Information Security

Since 1992, we have reviewed the effectiveness of IRS information security in connection with our annual audit of IRS's financial statements.[8] The results of these reviews have led us each year to designate information security as a material weakness.[9] We have also evaluated information security at IRS as a result of congressional requests. For example, in 1998, at the request of the Chairman and Ranking Minority Member of the Senate Committee on Governmental Affairs, we evaluated IRS's progress in correcting previously reported information security weaknesses.[10] We determined that although IRS had made significant progress in improving information security, serious weaknesses continued to exist at its facilities because the agency had not yet fully institutionalized its information security program. We recommended that IRS continue its actions to implement certain controls and to complete the implementation of an effective agencywide information security program.

We have also evaluated information security controls for IRS's electronic filing systems. The Chairman of the Senate Committee on Governmental Affairs requested that we assess the effectiveness of key computer controls designed to ensure the security, privacy, and reliability of IRS's electronic filing systems and electronically filed taxpayer information. In 2001, we reported that IRS had not adequately secured access to its electronic filing systems or to the electronically transmitted tax return information those systems contained during the 2000 tax filing season because IRS had not taken adequate steps to assess security risks and monitor the effectiveness of security controls on an ongoing basis.[11] We

[8]U.S. General Accounting Office, *Financial Audit: Examination of IRS's Fiscal Year 1992 Financial Statements*, GAO/AIMD-93-2 (Washington, D.C.: June 30, 1993).

[9]A material weakness is a condition that precludes the agency's internal controls from providing reasonable assurance that material misstatements in the financial statements would be prevented or detected on a timely basis.

[10]U.S. General Accounting Office, *IRS Systems Security: Although Significant Improvements Made, Tax Processing Operations and Data Still at Serious Risk*, GAO/AIMD-99-38 (Washington, D.C.: Dec. 14, 1998).

[11]U.S. General Accounting Office, *Information Security: IRS Electronic Filing Systems*, GAO-01-306 (Washington, D.C.: Feb. 16, 2001).

provided technical recommendations that addressed specific access control weaknesses and also recommended, among other things, that IRS implement procedures to assess risks and monitor the effectiveness of security controls over electronic filing systems on an ongoing basis. Last year, we again evaluated IRS's actions to resolve the information security weaknesses affecting its electronic filing systems and provided congressional testimony disclosing that IRS had substantially improved safeguards that controlled external access to its electronic filing systems and to the electronically transmitted tax return data those systems contained.[12] However, additional improvements were still needed to protect the electronically transmitted data on those systems from unauthorized access attempts by users of IRS's internal network.

Objectives, Scope, and Methodology

The objectives of our review were to (1) determine whether IRS has implemented effective computer controls to protect the confidentiality, integrity, and availability of sensitive systems and taxpayer data, and (2) determine whether IRS has fully implemented its agencywide information security program.

To determine the effectiveness of IRS computer controls and whether IRS had fully implemented its agencywide information security program, we considered the results of the 14 facility-specific general control reviews at 11 IRS facilities and 5 application control reviews[13] that we performed in connection with our audits of IRS's financial statements for fiscal years 1998 through 2001. We performed those reviews using the audit methodology described in our Federal Information System Controls Audit Manual,[14] which discusses the scope of such reviews and the type of testing required for evaluating computer controls intended to

- limit, detect, or monitor logical and physical access to sensitive computing resources and facilities, thereby protecting them from unauthorized disclosure, modification, and use;

[12]U.S. General Accounting Office, *Tax Administration: IRS Continues to Face Management Challenges in its Business Practices and Modernization Efforts*, GAO-02-619T (Washington, D.C.: Apr. 15, 2002).

[13]Although five applications were reviewed, only four application-specific reports were issued. One report contained the results of two application control reviews.

[14]U.S. General Accounting Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

- ensure that work responsibilities are segregated so that one individual does not perform or control key aspects of computer-related operations and thereby have the ability to conduct unauthorized actions or gain unauthorized access to assets or records;

- prevent unauthorized programs or modifications to existing programs from being implemented;

- minimize the risk of unplanned interruptions and recover critical computer processing operations if interruptions occur; and

- implement an agencywide information security program that includes a continuing cycle of assessing risk, implementing and promoting policies and procedures to increase awareness and reduce such risk, monitoring the effectiveness of those measures, and effectively coordinating those activities.

We consolidated and analyzed the information contained in reports of those reviews to determine, on an agencywide basis, the nature and extent of information security weaknesses affecting IRS systems and taxpayer data. We also assessed the sufficiency of IRS's information security policies and guidance by reviewing and comparing them with guidance issued by NIST, OMB, the National Security Agency (NSA), and certain vendors of software products used by IRS. In addition, we obtained and reviewed information-security-related documents and met with IRS security officials to discuss the status of efforts to correct reported weaknesses and fully implement the IRS information security program. We also tested and observed controls over certain network devices to determine whether IRS securely configured them to minimize the risk of unauthorized access.

Further, we determined the status of IRS actions to resolve reported information security weaknesses. We requested and evaluated written statements from IRS on actions taken to address recommendations made in the 14 facility-specific and 4 application-specific reports. We also conducted follow-up visits at four facilities to test the effectiveness of IRS's actions to resolve general control weaknesses identified in five reports.

Our review was performed at IRS headquarters and our headquarters in Washington, D.C., from September 2002 through March 2003, in accordance with generally accepted government auditing standards.

Although Improvements Made, Information Security Weaknesses Still Pose Risks

IRS has made important progress toward improving information security controls. It has acknowledged the seriousness of its information security weaknesses and the risks they pose to its operations, and has again designated information security as a material weakness in the Department of the Treasury's fiscal year 2002 accountability report.[15] It has also developed a plan of action and milestones to resolve the material weakness by March 31, 2004.

IRS has increased the resources devoted to securing its systems and data—increasing, for example, the number of specialists assigned to Security Services (formerly the Office of Systems Standards and Evaluation) from about 60 in 1998 to 97 in 2003. It has also implemented and improved control measures that limit physical access to facilities and computing resources, and has established a virus protection and eradication program, including regular updates from its software suppliers. Further, IRS now has a 24-hour-a-day, 7-day-a-week Computer Security Incident Response Capability team, which provides safeguards against various cyber threats. For example, IRS has installed firewalls and intrusion detection systems on its network, which the team monitors for security-related events. The agency also asserts that it has upgraded its headquarters continuity of operations plan and enhanced its master files disaster recovery capability.[16]

In addition, IRS is acquiring redundant communications capabilities to ensure that its executives have connectivity with the Department of the Treasury, law enforcement, and staff affected by incidents. It is also consolidating several of its geographically dispersed computer systems and centralizing responsibility for their operation and maintenance.

Although IRS has made important progress, it has not consistently implemented effective computer controls. Organizations can implement a number of different types of controls to protect computing resources. These include logical access controls—which ensure that only authorized individuals can read, alter, or delete data—and other information system

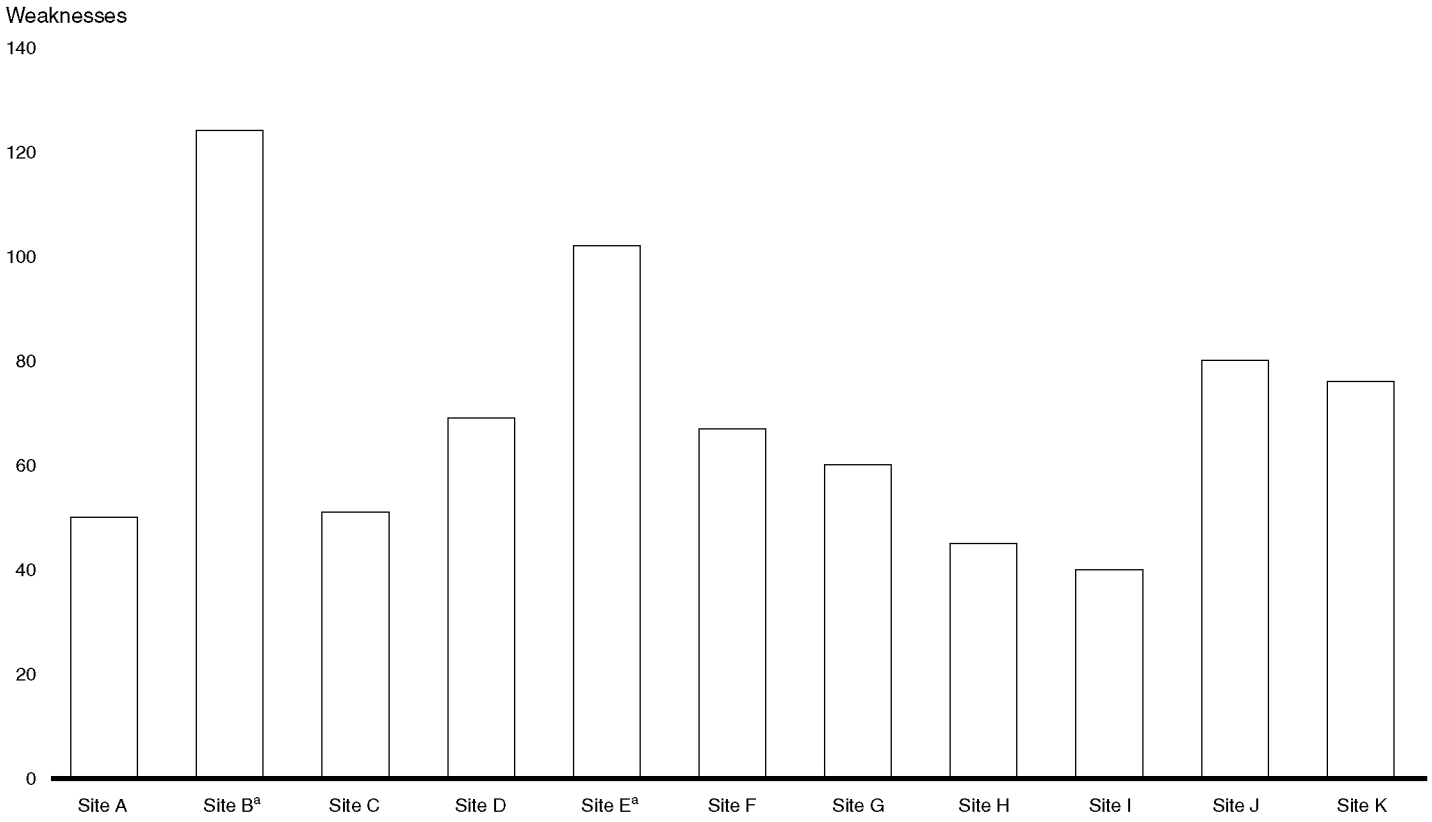
[15]The Federal Managers' Financial Integrity Act of 1982 (Public Law 97-255) requires the head of each agency to annually prepare a statement that identifies material weaknesses in the agency's systems of internal accounting and administrative control and its plans and schedule for correcting them.

[16]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.

controls. Such other controls include (1) physical security; (2) software change controls, which ensure that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; and (4) service continuity, which ensures that computer-dependent operations experience no significant disruptions.

However, computer-related weaknesses in these areas continued to pervade the IRS facilities we reviewed between 1999 and 2002. As figure 1 illustrates, many control weaknesses were found at each of the 11 facilities.

Figure 1: Number of Control Weaknesses Found at IRS Facilities



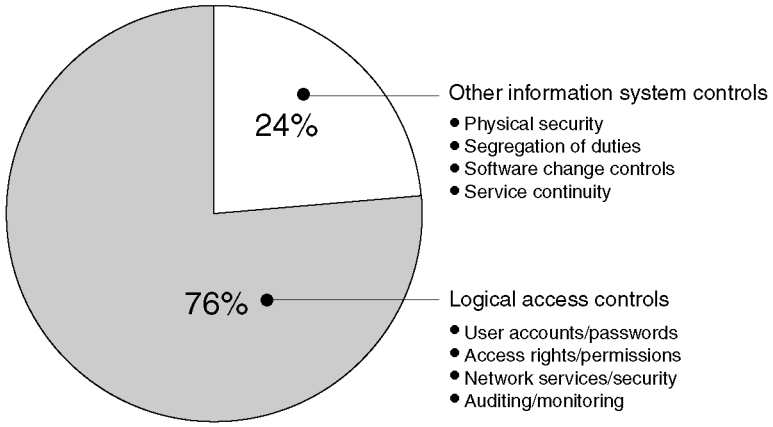
Source: GAO.

[a]We performed multiple reviews at these sites. The number of general control weaknesses indicated in this chart represents the total number of new weaknesses identified at each site during those reviews. Weaknesses were counted only once at each site. If a weakness was identified in a prior review but was not corrected and still existed during a subsequent review at the same site, it was not counted again.

Of the 14 general control reviews performed at the 11 facilities depicted in figure 1, 3 were done at site B, 2 at site E, and 1 at each of the remaining 9 sites. These reviews identified a total of 765 general control weaknesses at the 11 facilities. The number of new weaknesses identified in individual reviews ranged from 14 to 80, and averaged about 54. The large number of weaknesses at each IRS facility reviewed demonstrates that addressing information security is an agencywide challenge.

Moreover, weaknesses appeared in all general control categories, as illustrated in figure 2.

Figure 2: Breakdown of Weaknesses by General Control Category



Source: GAO.

The majority of the weaknesses appear in logical access controls. Although not as numerically significant as logical access controls, weaknesses in other information system controls were found at each IRS facility reviewed and also presented significant risk to IRS systems and taxpayer data.

Logical Access Controls Were Often Inadequate

IRS's implementation of logical access controls at its facilities does not effectively prevent, limit, or detect access to computing resources. A basic management objective for any organization is to protect its information systems and critical data from unauthorized access. Organizations accomplish this by designing and implementing logical access controls that are intended to prevent, limit, and detect unauthorized access to computing resources. These controls include user accounts and

passwords, access rights and permissions, network services and security, and audit and monitoring. Inadequate logical access controls diminish the reliability of computerized data and increase the risk of unauthorized disclosure, modification, and use of sensitive systems and taxpayer data.

User Accounts and Passwords

A computer system must be able to identify and differentiate among users so that activities on the system can be linked to specific individuals. Unique user accounts assigned to specific users allow systems to distinguish one user from another, a process called identification. The system must also establish the validity of a user's claimed identity through some means of authentication, such as a secret password, known only to its owner. The combination of identification and authentication, such as user account and password combinations, provides the basis for establishing individual accountability and controlling access to the system. Accordingly, agencies (1) implement procedures to control the creation, use, and removal of user accounts, and (2) establish password parameters, such as length, life, and composition, to strengthen the effectiveness of account and password combinations for authenticating the identity of users.

IRS did not adequately control user accounts and passwords to ensure that only authorized individuals were allowed access to computer systems. Weaknesses with the administration of user accounts and the configuration of password parameters created opportunities for individuals to masquerade as other users and potentially gain inappropriate access to computing resources, as the following examples illustrate.

- IRS did not always promptly remove inactive or unused accounts at any of the 11 facilities. Inactive accounts indicate that owners no longer need the access privileges provided by the accounts and may be attractive targets for individuals attempting to gain unauthorized access since the account owners may not notice illicit activity on the accounts.

- Users often created passwords that were common words or contained only alphabetic characters at eight facilities. The use of such passwords increases the possibility that someone could guess or crack the passwords based on personal knowledge of the users or through password-cracking software.

- IRS did not require passwords for certain accounts at eight facilities, significantly increasing the risk that unauthorized users could inappropriately utilize the access privileges provided by these accounts.

- IRS did not consistently configure certain password parameters securely, such as required password length and expiration, thereby increasing the risk that someone could guess the password and be able to use the compromised password for an extended period of time.

Weaknesses in controls over user accounts and passwords diminish the overall effectiveness of these controls in preventing individuals from gaining unauthorized access to computing resources and in tracing system activity back to the correct individual.

Access Rights and Permissions

A basic underlying principle for securing computer systems and data is the concept of least privilege. This means that users are granted only those access rights and permissions needed to perform their official duties. Organizations establish access rights and permissions to restrict the access of legitimate users to the specific programs and files that they need to do their work. User rights are allowable actions that can be assigned to users or groups. File and directory permissions are rules associated with a file or directory that regulate which users can access them and in what manner. Assignment of rights and permissions must be carefully considered to avoid giving users unintentional and unnecessary access to sensitive files and directories.

However, IRS did not sufficiently restrict user rights and file permissions on its computer systems. The agency sometimes granted access rights to users above and beyond those needed to perform their computer-related job responsibilities and created files with excessive file permissions, as the following examples illustrate.

- IRS inappropriately established excessive permissions for certain files at seven facilities. Files with these permissions can be modified by any user on the system, greatly increasing the risk that a user may, intentionally or inadvertently, make unauthorized changes to the file contents.

- IRS granted powerful operating system privileges to users who had no documented need for such rights at 10 facilities.

Inappropriate access to sensitive files and directories can enable a successful intruder or legitimate user to gain privileged administrator access to the system. This access also creates the possibility that users

might unintentionally modify or destroy system files. Such lapses can compromise the integrity of the operating system and the privacy of the data that reside on these systems.

Network Services and Security

Networks are series of interconnected devices and software that allow individuals to share data and computer programs. Because sensitive programs and data are stored on or transmitted along networks, effectively securing networks is essential to protecting computing resources and data from unauthorized access, manipulation, and use. Organizations secure their networks, in part, by limiting the services that are available on the network and by installing and configuring network devices that permit authorized network service requests and deny unauthorized requests. Network services consist of protocols for transmitting data between computers. Network devices include (1) firewalls designed to prevent unauthorized access into the network, (2) routers that forward data along the network, (3) switches that filter and forward information among parts of a network, and (4) servers that host applications and data. Insecurely configured network services and devices can make a system vulnerable to internal or external threats, such as denial-of- service attacks.[17] Since networks provide the entry point for access to electronic information assets, failure to secure them increases the risk of unauthorized use of sensitive data and systems.

IRS did not always securely control network services or configure devices to prevent unauthorized access to and ensure the integrity of computer systems operating on its networks. The agency enabled unnecessary, outdated, and misconfigured network services on certain servers and sometimes configured certain network devices in such a manner that it did not effectively reduce the risk of misuse or unauthorized access to computing resources on its networks, as the following examples demonstrate.

- Intruders could have gained valuable information about systems without logging in at 9 facilities.
- Insecure remote access existed on its systems at 10 facilities.

[17]A denial-of-service attack is an attack on a network that sends a flood of useless traffic that prevents legitimate use of the network.

- IRS was running easily exploitable and unnecessary services on servers at 10 facilities.

  Running vulnerable network services and insecurely configuring network devices increase the risk of system compromise, such as unauthorized access to and manipulation of sensitive system data, disruption of services, and denial of service.

Audit and Monitoring

Determining what, when, and by whom specific actions were taken on a system is crucial to establishing individual accountability, monitoring compliance with security policies, and investigating security violations. Organizations accomplish this by implementing system or security software that provides an audit trail for determining the source of a transaction or attempted transaction and monitoring users' activities. How organizations configure the system or security software determines the nature and extent of audit trail information that is provided. To be effective, organizations (1) configure the software to collect and maintain sufficient audit trail information[18] for security-relevant events;[19] (2) generate reports that selectively identify unauthorized, unusual, and sensitive access activity; and (3) regularly monitor and take action on these reports. Without sufficient auditing and monitoring, organizations increase the risk that they may not detect unauthorized activities or policy violations.

IRS did not consistently audit or monitor computer system activity. The agency did not (1) establish audit trails on some systems, (2) collect sufficient audit trail information on other systems, or (3) routinely review audit trail reports to monitor user activities on some systems to ensure that users were performing only authorized actions, as the following examples illustrate.

- IRS did not activate the system feature to collect audit trail information on key systems at 4 facilities.

[18]Audit trail information generally includes the (1) date and time the event occurred, (2) user ID associated with the event, (3) type of event, and (4) result of the event.

[19]Security-relevant events include (1) successful and unsuccessful log-on attempts; (2) log-offs; (3) change of password; (4) creation, deletion, opening, and closing of files; (5) all actions of users with privileged authority; and (6) program initiation.

- IRS did not capture all security-relevant events in audit logs on certain systems at 10 facilities.

- IRS did not adequately review audit information or monitor system activity on certain systems at 7 facilities. For example, agency personnel had not reviewed the audit configuration settings on certain systems to ensure that they produced complete audit records. Where records existed, they were not reviewed to determine if violations had occurred.

  As a result, increased risk exists that IRS may not detect unauthorized system activity or determine which users are responsible.

Other Information System Controls Were Also Inadequate

In addition to logical access controls, other important information system controls help ensure the confidentiality, integrity, and availability of systems and data at IRS facilities. These controls include policies, procedures, and techniques that physically secure data processing facilities and resources, properly segregate computing resources and incompatible duties among computer personnel, prevent unauthorized software changes, and effectively ensure the continuation of computer processing service if an unexpected interruption occurs. Despite the many information system controls that IRS has implemented, weaknesses in these areas increase the risk of unauthorized access, disclosure, and modification of data.

Physical Security

Physical security controls should be designed to prevent vandalism and sabotage, theft, accidental or deliberate alteration or destruction of information or property, attacks on personnel, and unauthorized access to computing resources. These controls include those that prevent, limit, and detect access to facility grounds, buildings, and sensitive work areas. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, and locks. On occasion, persons other than regularly authorized personnel may be granted access to facilities. An agency should control visitors using a variety of techniques, such as providing escorts, checking identification, requiring prior notice, and identifying visitors to staff by means of badges. Inadequate physical security could lead to the loss of life and property, the disruption of service and functions, and the unauthorized disclosure of documents and information.

Although IRS has implemented many physical security controls, certain weaknesses reduced their effectiveness in protecting and controlling

physical access to facility grounds, buildings, and sensitive work areas, as the following examples illustrate.

- Inadequate physical barriers, unlocked doors, or other control issues weakened perimeter security at 10 facilities.
- IRS did not always effectively screen visitors seeking access to certain facilities.
- At 8 facilities, as visitors left the premises, IRS did not consistently collect visitor badges to prevent subsequent unauthorized entry.

As a result, increased risk exists that unauthorized individuals could gain access to facility grounds, buildings, sensitive computing resources, and taxpayer data without detection.

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records. Often, segregation of duties is achieved by dividing responsibilities among two or more organizational groups. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed.

IRS did not consistently separate incompatible computer-related activities among individuals. For example, it did not sufficiently separate incompatible system administration and security administration duties at its facilities. To illustrate, it did not always divide among individuals the responsibility for adding and deleting systems users from the responsibility for maintaining system audit logs. IRS also assigned incompatible operating system privileges to users, such as granting auditing privileges to system administrators at 10 facilities. As a result, increased risk exists that errors or fraud could occur. For example, these individuals could add fictitious users with elevated access privileges and perform unauthorized system activity without detection.

Software Change Control

Also important for an organization's information security is ensuring that only authorized software programs are placed in operation. This is accomplished by instituting policies, procedures, and techniques that help make sure that all programs and program modifications are properly authorized, tested, and approved. To protect approved software programs from unauthorized changes, software development and test activities should not be performed on the same systems used to process production data and transactions. Moreover, access to programs should be restricted to authorized individuals only. Failure to do so increases the risk that unauthorized programs or changes could be, inadvertently or deliberately, placed into operation.

IRS did not institute sufficient controls over its software change procedures at some of the facilities reviewed to ensure that only authorized or current software programs were placed in operation. It also did not consistently protect software programs in the operating environment from the risk of unauthorized modification, as the following examples illustrate.

- IRS had not established sufficient control mechanisms at two facilities to ensure that the facilities received all of the program updates sent by the IRS national office.
- IRS personnel at one facility did not routinely perform post-implementation reviews of emergency software changes, as is required, to determine the propriety and effectiveness of the changes, thereby increasing the risk that unnecessary or unauthorized software was installed as emergency changes.
- Software developer accounts and/or software development tools were placed on production servers at five facilities. Such accounts and tools increase the risk that individuals could make unauthorized changes to the production software on these servers.

These software change control weaknesses at IRS facilities reduced the integrity and reliability of data processed by IRS systems.

Service Continuity

Service continuity controls should be designed to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected. These controls include (1) environmental controls and procedures designed to protect information resources and minimize the risk of unplanned interruptions and (2) a well-tested plan to recover critical

operations should interruptions occur. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information.

Although progress has been made, weaknesses in service continuity controls limit IRS's ability to restore and continue data processing service after a service disruption or emergency occurs. For example:

- IRS had not developed disaster recovery plans for certain key systems at seven facilities, thereby increasing the risk that IRS employees at these facilities would not know how to recover these systems and resume operations if unexpected disruptions occur.
- IRS had not adequately tested certain service continuity plans at five facilities, thereby reducing assurance that employees are adequately trained and planned procedures are sufficient to promptly recover and restore essential information systems and business operations.

As a result, IRS has diminished assurance that, in case of an unexpected interruption, it will be able to protect or recover essential information and critical business processes, potentially affecting its ability to accomplish its mission and serve taxpayers.

Application Controls Were Insufficient to Mitigate Risk

Application controls help ensure that transactions are valid, properly authorized, and completely and accurately processed by the computer. An application is a program, or group of programs, utilized by end-users to complete specific tasks, such as financial recording or payroll. Application controls include authorization controls that ensure that only authorized transactions by authorized users are entered into the system. Authorization controls are similar to logical access controls in that they help to ensure that (1) individual accountability is maintained, (2) only authorized transactions are processed, (3) the rights and privileges of users are limited to what is required for completing job-related duties, and (4) inappropriate or unauthorized activities are prevented or detected. For example, requiring users to enter account name/password combinations during log-on to the application helps ensure that only authorized users are accessing the application. Lack of such controls increases the risk that inaccurate or unauthorized transactions will be processed.

IRS did not consistently ensure that access to key computer applications was limited to authorized persons for authorized purposes. We reported 112 application control weaknesses during our reviews of five applications. Authorization control weaknesses, including those related to password controls, assigning access privileges, and monitoring user accounts, increased the risk of unauthorized disclosure, modification, or use of the applications and taxpayer data, as the following examples illustrate.

- Users created weak passwords on two of the five applications reviewed, thereby increasing the likelihood that someone could guess or crack their passwords.
- IRS granted certain employees rights and privileges that exceeded what their duties required on four applications reviewed.
- IRS did not always promptly revoke access rights of terminated employees to an application used for accessing taxpayer records.

As a result, increased risk exists that someone could gain unauthorized access to application and taxpayer data.

IRS Has Corrected Many Reported Weaknesses

IRS has made important progress in correcting the general and application control weaknesses that we reported on during the 3-year period ending July 31, 2002. We performed follow-up general control reviews for 5 of the 14 facility-specific reports issued during this period. On the basis of these follow-up reviews, we determined that IRS had corrected or mitigated the risk of just over half of the weaknesses (about 57 percent; 137 of 242). In addition, IRS asserts that it has corrected about a quarter of the weaknesses (about 23 percent; 122 of 523) identified in the remaining 9 reports. These corrective actions include (1) enhancing the effectiveness of IRS's network security controls that protect against external attempts to gain unauthorized access to IRS's internal systems and (2) enhancing, implementing, and testing the disaster recovery capability for the mission-critical master files. IRS has also corrected or mitigated the risk of over half (about 55 percent; 62 of 112) of the application control weaknesses reported for the 4 applications in the four application reports.

In addition, IRS has developed a plan of actions and milestones for resolving its material weakness in information security. The plan addresses the remaining work to be accomplished, which includes

- reexamining its security roles and responsibilities;
- analyzing security roles and responsibilities to assist it in developing implementation processes and improve accountability;
- improving its security criteria;
- mapping its policies and procedures to governmentwide security guidance to ensure the development of robust security criteria; and
- identifying, prioritizing, and certifying its sensitive systems.

The plan identifies (1) corrective actions, (2) the agency organization responsible for correcting the weakness, (3) key milestones with completion dates, and (4) the status of actions. It indicates that the planned completion date for resolving the material weakness is March 31, 2004, when IRS executives are scheduled to meet to validate the effectiveness of the corrective actions.

IRS Has Not Fully Implemented Elements of Its Agencywide Security Program

An underlying cause for the numerous weaknesses in information system controls at IRS facilities is that, although IRS has made progress, it has not fully implemented certain elements of its agencywide information security program. Our study of strong security management practices, as summarized in our 1998 Executive Guide,[20] found that leading organizations handle their information security risks through an ongoing cycle of risk management. This process involves (1) establishing a centralized management function to coordinate the continuous cycle of activities while providing guidance and oversight for the security of the organization as a whole; (2) assessing risks and determining what security measures are needed; (3) establishing and implementing policies and controls that meet those needs; (4) promoting security awareness so that users understand the risks and the related policies and controls in place to mitigate those risks; and (5) monitoring policies and controls to ensure that they are appropriate and effective and that known weaknesses are promptly mitigated.

[20]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

IRS has effectively implemented the first key element of the program: the Office of Security Services serves as the central focal point for coordinating, guiding, evaluating, and overseeing information security program activities. It has also taken steps to implement its agencywide program. For example, IRS has revised its information technology security policies and guidance to include the latest guidance on information security issued by OMB and NIST. It has also updated the specific security roles and responsibilities for its senior officials, managers, security personnel, and system users. In addition, IRS routinely reviews the effectiveness of information security at its facilities and is implementing automated tools to assist with the monitoring and auditing of the agency's computer systems. However, IRS has not yet fully or effectively implemented other elements of the program. These shortcomings undermine the agency's efforts to secure its facilities, systems, and sensitive data.

Assessing Risks and Determining Needs

Understanding the risks associated with information systems is a key element of an information security program. The Federal Information Security Management Act of 2002 and its predecessor, the Government Information Security Reform provisions,[21] require all federal agencies to develop comprehensive information security programs based on assessing and managing risks.[22] To help ensure that information systems are adequately protected from associated risks, federal organizations can perform risk assessments, develop system security plans, and formally authorize the use of each system before it becomes operational.

[21]When we performed our audit work, the two major laws related to federal computer information security that were in effect were the Computer Security Act, P. L. No. 100-235, January 8, 1988, and the Government Information Security Reform provisions (GISRA), Title X, Subtitle G, P. L. 106-398, October 30, 2000. Effective December 17, 2002, the Federal Information Security Management Act of 2002, Title III, P. L. 107-347, repealed GISRA and the Computer Security Act and replaced them with similar, but strengthened provisions.

[22]The February 1996 revision to OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, directs agencies to use a risk-based approach to determine adequate security, including a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. Additional guidance on effective risk assessment is available in NIST publications and in our *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D.C.: November 1999).

Risk Assessments

Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls. IRS policy requires that a risk assessment be performed at periodic intervals, commensurate with the sensitivity and criticality of data processed, but no less frequently than every 3 years if no assessment has been performed during that period.

However, at the time of our reviews, IRS had not assessed risks for many of its systems. According to the Treasury Inspector General for Tax Administration's Report on the Government Information Security Reform provisions for IRS for Fiscal Year 2002, only 34 percent of IRS's reported 305 sensitive systems had been assessed for risk. The lack of risk assessments indicates that IRS had not done all it was required to do to understand and manage risks to its systems. Inadequate assessment of risks can lead to the implementation of inadequate or inappropriate security controls that do not address the system's true risks and costly efforts to subsequently implement effective controls. According to IRS officials, they recognized the predicament caused by the long-standing practice of not assessing risks for individual systems. Until the risk assessments are complete, IRS officials stated that other risk management activities, such as on-site information security reviews and network scans to identify vulnerable systems, would assist in identifying risks. Also, under its information security plan of actions and milestones, IRS has an emphasis on certification and accreditation and is committed to have all its sensitive systems certified by 2004.

System Security Plans

Once a risk assessment has been performed, it can serve as a basis for defining system security requirements and identifying and selecting appropriate and cost-effective security controls. Federal information security laws and OMB Circular A-130, Appendix III, require that system security plans be prepared for all federal systems that contain sensitive information. The purpose of these plans is to (1) provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements; (2) delineate responsibilities and expected behavior of all individuals who access the system; and (3) serve as documentation of the structured process of planning adequate, cost-effective security protection for a system. IRS policy requires that all its applications and general support systems be covered by system security plans and that the plans be updated at least every 3 years or when significant changes to the systems occur. To facilitate consistency and ease in preparing system security plans, IRS has developed a comprehensive template that includes the required elements for a security plan.

IRS had not developed or updated system security plans for many of its systems. According to the Treasury Inspector General for Tax Administration's Report on the Government Information Security Reform provisions for IRS for Fiscal Year 2002, only 34 percent of IRS's reported 305 sensitive systems had an up-to-date security plan. Without current, comprehensive security plans, IRS has no assurance that all aspects of security have been considered in determining the security requirements of its sensitive systems and that adequate protection has been provided to meet those requirements.

System Authorization

OMB and IRS also require management officials to formally authorize the use of each general support system and major application before it becomes operational, when a significant change occurs, and at least every 3 years thereafter.[23] IRS employs a certification and accreditation process for authorizing the use of its systems and applications. System certification is based on a technical evaluation of an information system to see how well it meets its security requirements, including all applicable federal laws, policies, regulations, and standards. System accreditation is the written management authorization for a system to operate and/or process information. IRS requires that this authorization be based on a complete and reliable assessment of the management, operational, and technical controls that are in place to mitigate the vulnerabilities to which the system is exposed, and assurance that the controls function as intended. In addition, IRS requires that a risk assessment, contingency plan, system security plan, and rules of behavior have been developed and are in place before a system can be authorized for processing.

However, IRS managers had not authorized the use of many of IRS's systems. According to the Department of the Treasury's 2002 annual program review required by the Government Information Security Reform provisions (P.L. 106-398), only about 35 percent of IRS's sensitive systems have been authorized for processing following the completion of system certification and accreditation. Thus, about 65 percent of IRS's sensitive systems were deployed and operating without written management authorization and, potentially, without the benefit of a comprehensive assessment of their security controls. The lack of authorization indicates that systems' managers have not reviewed and accepted responsibility for the adequacy of the security controls implemented on their systems and

[23]Authorization is sometimes referred to as accreditation.

increases the risk that systems will be deployed with security vulnerabilities.

The risks associated with not certifying and accrediting systems are particularly significant for IRS since many of its systems are designed and developed centrally at one facility and then deployed for operation at multiple facilities. Thus, the deployment of a centrally developed, insecurely configured system may introduce security vulnerabilities at multiple facilities. Indeed, personnel at the IRS facilities reviewed stated that information systems were deployed with some of the insecure system configurations identified during our tests.

Establishing and Implementing Policies and Controls

Another key element of an effective information security program, as identified during our study of information security management practices at leading organizations, is establishing and implementing appropriate policies and related controls. Establishing or documenting security policies is important because they are the primary mechanism by which management communicates its views and requirements and serve as the basis for adopting specific procedures and technical controls. In addition, agencies need to take the actions necessary to effectively implement or execute these procedures and controls. Otherwise, agency systems and information will not receive the protection provided by the security policies and controls.

IRS has established a substantial set of information security policies, standards, and guidelines that generally provides appropriate guidance to personnel responsible for securing IRS information systems and data. Yet, there were instances in which security policies or implementing guidelines for certain systems either did not address certain security controls or were not consistent with strong security practices. These shortcomings pertained to the configuration and use of certain network services and devices, password parameters (such as password age and length), and the assignment of certain operating system rights. Overall, though, IRS has established information security policies, standards, and guidelines that, if effectively implemented, would protect its information systems from many threats.

Effective implementation and compliance have, however, been a problem. IRS routinely did not effectively implement or comply with its policies, standards, and guidelines for securing information systems. About 30 percent of all weaknesses we reported during the 3-year period existed because IRS personnel did not perform procedures, configure systems, or

implement controls in accordance with IRS policies and guidelines. Moreover, about half of the weaknesses identified during our three most recent information security reviews were the result of IRS personnel not implementing established policies and guidelines. Implementing and complying with appropriate information security policies, standards, and guidelines are essential elements of an effective security program.

Two factors contributed to the creation of these security weaknesses. First, the procedures IRS established to certify and accredit its systems are designed to ensure that the systems comply with established security policies and standards. However, as discussed, IRS's historically inconsistent performance in certifying and accrediting its information systems may have resulted in the deployment of systems that were not configured in accordance with agency policies and standards. Second, the agency has not established sufficient methods for holding personnel accountable for implementing security policies and controls. According to an IRS official, performance standards and measures that address compliance with information security policies have not been incorporated into performance appraisal mechanisms for IRS executives, managers, and users. Until such performance standards and measures are developed and incorporated into the appraisal process, agency personnel may not devote sufficient attention and effort to implementing effective security controls. The inconsistent application of security policies and controls increases the risk that unauthorized access, loss, or manipulation of sensitive systems and data may occur.

Promoting Security Awareness and Training

Another important element of an information security program involves promoting awareness and providing required training so that users understand the risks and their role in implementing related policies and controls to mitigate those risks. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital that employees who use computer systems in their day-to-day operations be aware of the importance and sensitivity of the information they handle, as well as the business and legal reasons for maintaining its confidentiality, integrity, and availability. OMB Circular A-130, Appendix III, provides that employees be trained on how to fulfill their security responsibilities before being allowed access to sensitive systems. Federal information security laws mandate that all federal employees and contractors involved with the management, use, or operation of federal computer systems be provided periodic training in information security awareness and accepted information security practice.

IRS has developed and implemented several methods for notifying employees of their security-related responsibilities. These include specifying security roles and responsibilities in various policy manuals and documents available to employees, requiring computer users to certify that they understand the system security rules for all information systems to which they have been granted access, and requiring each employee to receive a mandatory annual awareness briefing that focuses on the protection against and prevention of willful unauthorized access and inspection of taxpayer returns or tax return information.

However, the extent of noncompliance with IRS security policies and guidelines suggests that some IRS employees are either unaware of their responsibilities or insensitive to the need for implementing important information system controls. Although IRS had specified security roles and responsibilities in policy manuals, it had not, at the time of our reviews, linked them to executive, manager, and user positions in IRS's operating divisions. According to IRS security officials, some operating division managers had inappropriately believed that implementing security controls on their systems was not their responsibility but, rather, was the responsibility of Security Services personnel. In addition, IRS did not consistently provide sufficient security-related training to key security personnel. For example, security administrators at four IRS facilities possessed limited knowledge, and had not received training, about certain technical controls of system software they monitored. Insufficient technical security knowledge among key security personnel increases the risk that they will not promptly detect and mitigate security weaknesses.

Monitoring the Effectiveness of Controls and Mitigating Weaknesses

The final key element of an information security program is ongoing testing and evaluation to ensure that systems are in compliance with policies, and that policies and controls are both appropriate and effective. This type of oversight is a fundamental element because it demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. For these reasons, OMB Circular A-130, Appendix III, directs that the security controls of major information systems be independently reviewed or audited at least every 3 years. Although monitoring in itself may encourage compliance with security policies, the full benefits of monitoring are not achieved unless the results improve the security program. Analyzing the results of monitoring efforts, as well as security reviews performed by external audit organizations, provides security specialists and business managers with a means of (1)

identifying new problem areas, (2) reassessing the appropriateness of existing controls, and (3) identifying the need for new controls.

The IRS Office of Security Services has established a program for reviewing and evaluating controls over IRS's information systems. During fiscal year 2002, IRS reported that it performed 258 information security reviews at key facilities, including computing centers, development centers, campuses, and area offices. These included physical security reviews, operations reviews, communications security reviews, disaster recovery/business resumption reviews, and technical control reviews over its mainframe, Unix, and Windows NT systems.

However, IRS did not always take full advantage of review or audit results to proactively improve security controls at its facilities. Specifically, it did not take sufficient steps to ensure that weaknesses identified at one facility were promptly considered and addressed at other facilities. Our reviews have consistently identified weaknesses at IRS facilities that were previously identified at other facilities. About 61 percent of the weaknesses identified during the 3-year period covered by this report were found at more than one facility. For example, nine facilities allowed access to certain system information without requiring a log-on. We first reported this weakness at a facility in 1999 and continued to report it at other facilities through 2001. Further, IRS sometimes did not act to ensure that weaknesses identified on one system were considered and addressed on other similar systems at the same facility. For example, during a follow-up review at one facility, an IRS official said he believed that the facility had effectively corrected certain previously reported vulnerabilities because facility employees had corrected the vulnerabilities on the specific systems that were evaluated during the prior review. However, they did not consider or correct the same vulnerabilities on other similar systems that were not included in the prior review.

As weaknesses are identified, it is important to determine whether those weaknesses exist on similar systems at the same facility or at other facilities because of the degree of standardization that exists among similar systems and facilities. The lack of sufficient procedures to proactively ensure that weaknesses found at an IRS facility or on a system are considered and, if necessary, corrected at other facilities or on similar systems could lead to a false sense of security and expose IRS systems and data to increased, unnecessary risks.

IRS Is Taking Action to Improve Its Information Security Program

IRS has acknowledged the seriousness of its information security weaknesses and is taking action to improve its agencywide information security program. The program is in transition from a facility-based approach to an enterprise-based approach, which is aligned with IRS's reorganized operating divisions and the centralized information management within Modernization, Information Technology, and Security Services. This approach, led by Security Services, depends on the support of various IRS organizations to implement and monitor corrective actions. This includes defining specific security roles and responsibilities for executive, manager, and user positions throughout the agency, including those in the operating divisions. Ongoing efforts to adequately mitigate weaknesses are primarily focused on developing and implementing consistent security procedures for all operating divisions, ensuring day-to-day execution of these procedures, and certifying the backlog of uncertified systems.

However, until IRS can fully implement an effective agencywide information security program and adequately mitigate its information security weaknesses, it will remain at heightened risk of access to critical hardware and software by unauthorized individuals, who could intentionally or inadvertently add, alter, or delete sensitive data or computer programs. Such individuals could possibly obtain personal taxpayer information and use it to commit financial crimes in the taxpayer's name (identity fraud), such as establishing credit and incurring debt.

Conclusions

IRS has made important progress toward improving information security controls and implementing an agencywide information security program. Yet, much work remains to be done to resolve significant control weaknesses that continue to exist within its computing environment and to enable IRS to promptly address new security threats and risks as they emerge. We have previously provided IRS with many detailed recommendations for mitigating the individual weaknesses summarized in this report. Ensuring that known weaknesses affecting IRS's computing resources are promptly mitigated and that computer controls effectively protect its systems and data requires support and leadership from senior management of IRS's information technology and operating divisions, disciplined processes, and consistent oversight. Implementing an effective agencywide information security program requires that IRS take a comprehensive approach that includes assessing risks and evaluating needs, establishing and implementing appropriate policies and controls, enhancing awareness and technical skills, and monitoring the

effectiveness of controls on an ongoing basis. Further, a successful program will need the active and accountable involvement of both (1) operating division executives and managers who understand which aspects of their missions and information systems are the most critical and sensitive and (2) technical experts who know the agencies' systems and understand the technical aspects of implementing security controls. Until IRS effectively and fully implements its agencywide information security program, assurance will remain limited that IRS's financial information and taxpayers' personal information are adequately safeguarded against unauthorized use, disclosure, and modification, and its exposure to these risks will remain unnecessarily high.

Recommendations for Executive Action

To implement an effective agencywide information security program, we recommend that the IRS Commissioner direct the Chief Information Officer and the senior management official of each operating division to do the following:

- Assess risks and evaluate security needs by
  - performing risk assessments for all systems;
  - developing security plans for all systems; and
  - certifying and accrediting all systems before they become operational, upon significant change, and at least every 3 years thereafter.
- Establish and implement adequate information security policies and controls by
  - updating security policies or implementing guidelines pertaining to the configuration and use of certain network services and devices, password parameters, and the assignment of certain operating system rights, to be consistent with strong security practices;
  - testing and assessing security controls and configurations of systems before deployment for compliance with established security policies and standards; and
  - establishing and incorporating performance standards for compliance with security policies and procedures in the performance appraisal process for IRS executives and managers in the information technology and operating divisions.
- Enhance information security awareness and training programs by

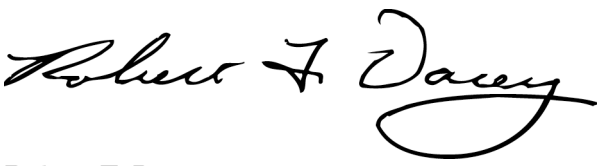
- providing training to IRS employees and contractors, including executives, managers, and users, and including those in the information technology and operating divisions, on their security roles and responsibilities; and
- providing security-related training commensurate with job-related responsibilities to security personnel.

- Monitor the effectiveness of controls and mitigate known information security weaknesses by establishing and implementing procedures to proactively ensure that weaknesses found at an IRS facility or on a system are considered and, if necessary, corrected at other facilities or on similar systems.

Agency Comments

In providing written comments on a draft of this report (which are reprinted in appendix I), the Commissioner of Internal Revenue generally agreed with the report, and indicated that IRS is acting to implement our recommendations. The Commissioner noted that safeguarding taxpayer information is one of IRS's highest priorities and that the agency continues to strengthen its security controls. According to the Commissioner, IRS is taking several steps to (1) assess risk and evaluate its security needs, (2) establish and consistently implement information security policies and controls, (3) implement a computer security training program, and (4) develop executive-level feedback mechanisms to monitor the effectiveness of controls to ensure that corrective actions are implemented on an enterprisewide basis.

If you have any questions or need further information about the material contained in this report, please contact Gregory C. Wilshusen, Assistant Director, at (202) 512-6244, or me at (202) 512-3317. We can also be reached by E-mail at wilshuseng@gao.gov or daceyr@gao.gov, respectively. Other key contributors to this report include Ramnik Dhaliwal, Suzanne Lightman, and Evelyn Logue.



Robert F. Dacey
Director, Information Security Issues

Appendix I: Comments from the Internal Revenue Service

COMMISSIONER

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

May 16, 2003

Mr. Robert F. Dacey
Director, Information Security Issues
U.S. General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Dacey:

I have reviewed the General Accounting Office (GAO) report entitled, Information Security: Although Progress Made, Weaknesses at the Internal Revenue Service Continue to Pose Risks, (GAO-03-44, May 2003). I assure you that safeguarding taxpayer information is one of our highest priorities. As you acknowledged in this report, we have continued to strengthen important security controls throughout the three year review period as GAO brought audit findings to our attention.

Since 1997, GAO has designated information security as a government-wide, high-risk area. In 1997, we established a facility-based approach to secure our physical environment and to focus on resolving vulnerabilities of our most critical tax processing systems and data. The GAO acknowledged that we implemented many significant corrective actions under this approach, but that several internal control weaknesses continue to exist. In this report, you indicated we have adequately mitigated external physical vulnerabilities, but that we need to continue to focus on the internal vulnerabilities of our systems.

We agree with this assessment and as a result, in FY2002, we began transitioning the security program from a facility-based approach to an enterprise-based approach, which is aligned with our reorganized business units and the centralized information management within Modernization, Information Technology and Security Services (MITSS). This approach relies on the involvement of the IRS leadership and managers, and focuses on identifying, mitigating, and resolving control risks throughout the IRS by implementing consistent and appropriate security policies, training, and monitoring processes. We believe this approach will improve our overall security program and mitigate much of the identified computer security weaknesses.

This report focuses on resolving inconsistencies and making needed improvements. However, I would like to mention some of the many accomplishments of the security

program over the last eighteen months that have significantly strengthened the security of the IRS and improved consistency in many security-related areas. These accomplishments include:

- Improved physical security controls at data processing facilities
- Improved campus and mailroom capabilities by enhancing mail handling locations, operations, and training
- Enhanced decision support capabilities by implementing four Situation Awareness and Management Centers that provide daily reports on physical and cyber incidents to the IRS senior leaders
- Upgraded and tested the Headquarters' Continuity of Operations Plan (COOP)
- Enhanced disaster recovery capability for the Masterfile by establishing an in-house capability
- Improved controls, updated standards, and installed security upgrades for mainframe systems, mid-level computing environments, and electronic filing systems

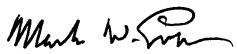
In addition, we strengthened our computer security capabilities by establishing important operational capabilities to safeguard against hacking and terrorist threats. We maintain a virus protection and eradication program, which includes regular updates from virus software suppliers. This program is tightly integrated with our 24X7 Computer Security Incident Response Capability (CSIRC) team, which protects our network and systems against various cyber threats. In this regard, we can quickly respond to external and internal electronic intrusions to our infrastructure.

During the remainder of FY2003 and FY2004 our primary focus will be to continue implementing strong security measures and mitigating computer security material weaknesses. We analyzed previous GAO findings on the computer security material weakness, and identified nine specific areas needing improvement. These nine areas are being addressed in the Plan of Actions and Milestones (POA&M) report that we use to monitor progress by activity and responsible organization. We are also using the Treasury Security Assessment Framework to prioritize actions, track progress, and quantify success. We expect to significantly improve the consistent implementation of security controls by December 2003.

In August and December 2002, and most recently in April 2003, IRS representatives met with GAO and the Treasury Inspector General for Tax Administration on the specific actions needed to demonstrate the adequacy of our material weakness mitigation approach, and presented the POA&M. We received GAO's concurrence on our strategy. I have enclosed a description of how this material weakness mitigation strategy and other efforts address the Recommendations for Executive Actions.

These report findings, along with GAO's assistance, have been instrumental in supporting our continuing efforts to improve our computer security capabilities. If you have any questions, or if you would like to discuss this response in more detail, please contact me or Dave A. Mader, Acting Deputy Commissioner, Modernization, Information Technology and Security Services at (202) 622-6800.

Sincerely,



Mark W. Everson

Enclosure

The following information outlines the major components of IRS' security program that address each of GAO's specific recommendations for executive action:

1. IRS' security program includes continuous activities that assess risk and evaluate security needs by:
   a. Conducting security compliance reviews of logical information technology controls, physical facility controls, personnel security controls, and continuity of operations capability at all computing centers, campuses, and other computer locations that support major financial systems and infrastructure. For FY2003, we will implement throughout the agency the National Institute of Standards and Technology security self-assessment, a component of the Federal Information Security Management Act
   b. Ensuring that security plans are developed to assess the risk level of each sensitive system in accordance with acceptable certification and accreditation criteria
   c. Identifying and prioritizing all sensitive systems for certification and accreditation, monitoring for re-certification, and reducing the current backlog of uncertified systems (scheduled to be 75% completed by September 30, 2003 and 100% complete by September 30, 2004)

2. IRS' corrective action plan to mitigate computer security material weakness will consistently establish and implement adequate information security policies and controls to:
   a. Adequately restrict electronic access to and within computer network operational components by issuing appropriate guidelines, standards, and procedures, as well as a change control process for network standards
   b. Adequately ensure that access to key computer applications and systems is limited to authorized persons for authorized purposes by issuing new and updated computer and physical access controls, and personnel security requirements
   c. Consistently implement configuration and change control management processes to optimally configure system software to ensure the security and integrity of system programs, files, and data, and include testing and assessing of security controls before deploying systems
   d. Effectively monitor key networks and systems to identify unauthorized activities and inappropriate system configurations by deploying auditing standards, procedures, and notification processes

   In addition, IRS will develop and incorporate a written performance standard to address executive and manager responsibilities for effective security controls for all activities under their jurisdiction. This performance standard will be included

as a "Commitment" in all FY2004 executive performance plans. (Because an employee must serve a minimum of 120 days under a standard before he/she can be rated against it, we cannot implement a security standard for the FY2003 performance period, which ends on September 30.)

3. IRS' corrective action plan for computer security material weakness will consistently establish, enhance, and implement an adequate computer security training program by:
    a. Appropriately define security roles and responsibilities for executives, managers, users, system administration, security administration, database administration, user administration, operations, and software development, including contractors, as well as develop appropriate security awareness and training mechanisms
    b. Sufficiently provide security awareness and technical security-related training commensurate with the daily duties of key personnel through an updated and targeted security curriculum for information security professionals

4. IRS' corrective action plan for computer security material weakness will include executive level feedback mechanisms to monitor effectiveness of controls and to mitigate known weakness to ensure that we:
    a. Provide reports and metrics to accountable executives on the state of compliance with security controls that have an enterprise-wide impact
    b. Apply appropriate corrective actions enterprise-wide for consistent implementation and stronger overall security controls.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER