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.

May 2003

INFORMATION SECURITY

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

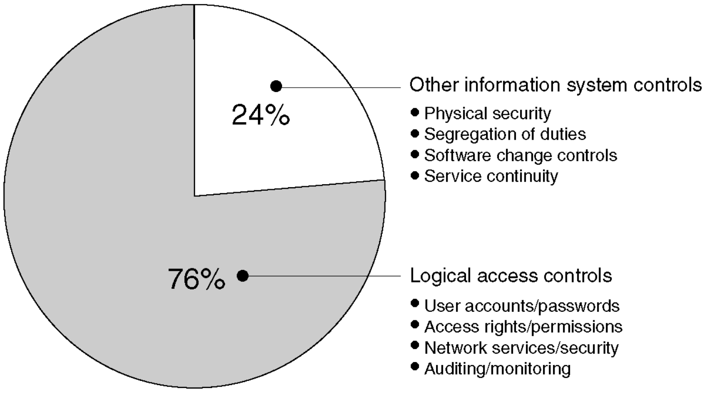
What GAO Found

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.