



Highlights of [GAO-07-364](#), a report to the Commissioner of Internal Revenue

## Why GAO Did This Study

In fiscal year 2006, the Internal Revenue Service (IRS) collected about \$2.5 trillion in tax payments and paid about \$277 billion in refunds. Because IRS relies extensively on computerized systems, effective information security controls are essential to ensuring that financial and taxpayer information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As part of its audit of IRS's fiscal years 2006 and 2005 financial statements, GAO assessed (1) IRS's actions to correct previously reported information security weaknesses and (2) whether controls were effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. To do this, GAO examined IRS information security policies and procedures, guidance, security plans, reports, and other documents; tested controls over five critical applications at three IRS sites; and interviewed key security representatives and management officials.

## What GAO Recommends

GAO is recommending that the IRS Commissioner take several actions to fully implement an agencywide information security program. In commenting on a draft of this report, IRS agreed to address all recommendations.

[www.gao.gov/cgi-bin/getrpt?GAO-07-364](http://www.gao.gov/cgi-bin/getrpt?GAO-07-364).

To view the full product, including the scope and methodology, click on the link above. For more information, contact Greg Wilshusen at (202) 512-6244 or [WilshusenG@gao.gov](mailto:WilshusenG@gao.gov) or Keith A. Rhodes at (202) 512-6412 or [Rhodesk@gao.gov](mailto:Rhodesk@gao.gov).

## INFORMATION SECURITY

# Further Efforts Needed to Address Significant Weaknesses at the Internal Revenue Service

## What GAO Found

IRS has made limited progress toward correcting or mitigating previously reported information security weaknesses at two data processing sites, but 66 percent of the weaknesses that GAO had previously identified still existed. Specifically, IRS has corrected or mitigated 25 of the 73 information security weaknesses that GAO reported as unresolved at the time of our last review. For example, IRS has improved password controls on its servers and enhanced audit and monitoring efforts for mainframe and Windows user activity, but it continues to (1) use inadequate account lockout settings for Windows servers and (2) inadequately verify employees' identities against official IRS photo identification.

Significant weaknesses in access controls and other information security controls continue to threaten the confidentiality, integrity, and availability of IRS's financial and tax processing systems and information. For example, IRS has not implemented effective access controls related to user identification and authentication, authorization, cryptography, audit and monitoring, physical security, and other information security controls. These weaknesses could impair IRS's ability to perform vital functions and increase the risk of unauthorized disclosure, modification, or destruction of financial and sensitive taxpayer information. Accordingly, GAO has reported a material weakness in IRS's internal controls over its financial and tax processing systems.

A primary reason for the new and old weaknesses is that IRS has not yet fully implemented its information security program. IRS has taken a number of steps to develop, document, and implement an information security program. However, the agency has not yet fully or consistently implemented critical elements of its program. Until IRS fully implements an agencywide information security program that includes risk assessments, enhanced policies and procedures, security plans, training, adequate tests and evaluations, and a continuity of operations process for all major systems, the financial and sensitive taxpayer information on its systems will remain vulnerable.