March 2010

INFORMATION SECURITY

IRS Needs to Continue to Address Significant Weaknesses

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-355, a report to the Commissioner of Internal Revenue

Why GAO Did This Study

The Internal Revenue Service (IRS) relies extensively on computerized systems to carry out its demanding responsibilities to collect taxes, process tax returns, and enforce the nation's tax laws. Effective information security controls are essential to protect financial and taxpayer information from inadvertent or deliberate misuse, improper disclosure, or destruction.

As part of its audit of IRS's fiscal years 2009 and 2008 financial statements, GAO assessed (1) the status of IRS's actions to correct or mitigate previously reported information security weaknesses and (2) whether controls over key financial and tax processing systems are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. To do this, GAO examined IRS information security policies, plans, and procedures; tested controls over key financial applications; and interviewed key agency officials at six sites.

What GAO Recommends

GAO is recommending that IRS take four actions towards fully implementing its agencywide information security program. In a separate report with limited distribution, GAO recommends 23 specific actions for IRS to take in correcting newly identified control weaknesses. In commenting on a draft of this report, IRS agreed to develop a detailed corrective action plan addressing each of the recommendations.

View GAO-10-355 or key components. For more information, contact Nancy Kingsbury at (202) 512-2700 or kingsburyn@gao.gov or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

IRS has continued to make progress during fiscal year 2009 in correcting previously reported information security weaknesses that GAO reported as unresolved at the conclusion of its fiscal year 2008 audit. Specifically, IRS has corrected or mitigated 28 of the 89 weaknesses and deficiencies—21 of 74 previously identified information security control weaknesses and 7 of 15 previously identified program deficiencies. For example, it has

- changed vendor-supplied user accounts and passwords;
- avoided storing clear-text passwords in scripts;
- enhanced its policies and procedures for configuring mainframe operations; and
- established an alternate processing site for its procurement system.

While IRS has corrected 28 control weaknesses and program deficiencies, 61 of them—or about 69 percent—remain unresolved or unmitigated. For example, IRS continued to install patches in an untimely manner and used passwords that were not complex. In addition, IRS did not always verify that remedial actions were implemented or effectively mitigated the security weaknesses. According to IRS officials, they continued to address uncorrected weaknesses and, subsequent to GAO's site visits, had completed additional corrective actions on some of them.

Despite these actions, newly identified and the unresolved information security control weaknesses in key financial and tax processing systems continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information. IRS did not consistently implement controls that were intended to prevent, limit, and detect unauthorized access to its systems and information. For example, IRS did not always (1) enforce strong password management for properly identifying and authenticating users; (2) authorize user access to permit only the access needed to perform job functions; (3) log and monitor security events on a key system; and (4) physically protect its computer resources. A key reason for these weaknesses is that IRS has not yet fully implemented its agencywide information security program to ensure that controls are appropriately designed and operating effectively. Although IRS has made important progress in developing and documenting its information security program, it did not, among other things, review risk assessments at least annually for certain systems or ensure contractors receive awareness training. Until these control weaknesses and program deficiencies are corrected, the agency remains unnecessarily vulnerable to insider threats related to the unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as the disruption of system operations and services. The new and unresolved weaknesses and deficiencies are the basis for GAO's determination that IRS had a material weakness in internal controls over financial reporting related to information security in fiscal year 2009.