January 2008

INFORMATION SECURITY

IRS Needs to Address Pervasive Weaknesses

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-211, a report to the Acting 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 (about $2.7 trillion in fiscal year 2007), process tax returns, and enforce the nation's tax laws. 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 2007 and 2006 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 key financial applications at three IRS data centers; and interviewed key security representatives and management officials.

What GAO Recommends

GAO is recommending that the Acting Commissioner take several actions to fully implement an agencywide information security program. In commenting on a draft of this report, IRS agreed to develop a detailed corrective action plan addressing each of the recommendations.

To view the full product, including the scope and methodology, click on GAO-08-211. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Nancy Kingsbury at (202) 512-2700 or kingsburyn@gao.gov.

What GAO Found

IRS made limited progress toward correcting previously reported information security weaknesses. It has corrected or mitigated 29 of the 98 information security weaknesses that GAO reported as unresolved at the time of its last review. For example, IRS implemented controls for user IDs for certain critical servers, improved physical protection for its procurement system, developed a security plan for a key financial system, and upgraded servers that had been using obsolete operating systems. In addition, IRS established enterprisewide objectives for improving information security, including initiatives for protecting and encrypting data, securing information technology assets, and building security into new applications. However, about 70 percent of the previously identified information security weaknesses remain unresolved. For example, IRS continues to, among other things, use passwords that are not complex, grant excessive access to individuals who do not need it, and install patches in an untimely manner.

In addition to this limited progress, other significant weaknesses in various controls continue to threaten the confidentiality and availability of IRS's financial processing systems and information, and limit assurance of the integrity and reliability of its financial and taxpayer information. IRS has not consistently implemented effective controls to prevent, limit, or detect unauthorized access to computing resources from within its internal network. For example, IRS did not always (1) enforce strong password management for properly identifying and authenticating users, (2) authorize user access to only permit access needed to perform job functions, (3) encrypt sensitive data, (4) effectively monitor changes on its mainframe, and (5) physically protect its computer resources. In addition, IRS faces risks to its financial and taxpayer information due to weaknesses in implementing its configuration management policies, as well as appropriately segregating incompatible job duties. Accordingly, GAO has reported a material weakness in IRS's internal controls over its financial and tax processing systems. A key reason for the weaknesses is that the agency has not yet fully implemented its agencywide information security program to ensure that controls are effectively established and maintained. As a result, IRS is at increased risk of unauthorized disclosure, modification, or destruction of financial and taxpayer information.