April 14, 2016

INFORMATION SECURITY

IRS Needs to Further Enhance Controls over Taxpayer and Financial Data

GAO

Highlights

Highlights of GAO-16-590T, a testimony before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives

Why GAO Did This Study

In collecting taxes, processing returns, and providing taxpayer service, IRS relies extensively on computerized information systems. Accordingly, it is critical that sensitive taxpayer and other data are protected. Recent data breaches at IRS highlight the vulnerability of taxpayer information. In addition, identity theft refund fraud is an evolving threat that occurs when a thief files a fraudulent tax return using a legitimate taxpayer's identity and claims a refund.

Since 1997, GAO has designated federal information security as a government-wide high-risk area, and in 2015 it expanded this area to include the protection of personally identifiable information. GAO also added identity theft refund fraud to its high-risk area on the enforcement of tax laws.

This statement discusses (1) IRS's information security controls over tax processing and financial systems and (2) roles that federal agencies with government-wide information security responsibilities play in providing guidance and oversight to agencies. This statement is based on previously published GAO work and a review of federal guidance.

What GAO Recommends

In addition to 49 prior recommendations that had not been implemented, GAO made 45 new recommendations to IRS in March 2016 to further improve its information security controls and program. GAO also recommended that IRS assess costs, benefits, and risks of taxpayer authentication options.

View GAO-16-590T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or James R. McTigue, Jr. at (202) 512-9110 or mctiguej@gao.gov.

What GAO Found

In March 2016 GAO reported that the Internal Revenue Service (IRS) had instituted numerous controls over key financial and tax processing systems; however, it had not always effectively implemented safeguards intended to properly restrict access to systems and information. In particular, while IRS had improved some of its access controls, weaknesses remained with identifying and authenticating users, authorizing users' level of rights and privileges, encrypting sensitive data, auditing and monitoring network activity, and physically securing its computing resources. These weaknesses were due in part to IRS's inconsistent implementation of its agency-wide security program, including not fully implementing GAO recommendations. The table below shows the status of prior and new GAO recommendations as of the end of its fiscal year (FY) 2015 audit of IRS's information security. GAO concluded that these weaknesses collectively constituted a significant deficiency for the purposes of financial reporting for fiscal year 2015. Until they are effectively mitigated, taxpayer and financial data will continue to be exposed to unnecessary risk.

Status of GAO Information Security Recommendations to IRS as of March 2016

Information security control area	Prior GAO recommendations open at the start of FY 2015 audit	Recommendations closed during FY 2015 audit	New recommendations	Outstanding recommendations at end of FY 2015 audit
Information security program	12	(3)	2	11
Access controls	34	(11)	38	61
Other controls	24	(7)	5	22
Totals	**70**	**(21)**	**45**	**94**

Source: GAO analysis of IRS data. | GAO-16-590T

The importance of protecting taxpayer information is further highlighted by the billions of dollars that have been lost to identity theft refund fraud, which continues to be an evolving threat. While IRS has taken steps to address this issue, as GAO reported in January 2015 it has yet to assess the costs, benefits, and risks of methods for improving the authentication of taxpayers' identity.

The Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) provide government-wide guidance and oversight for federal information security. These agencies have taken a number of actions to carry out these responsibilities. For example:

- OMB has prescribed security policies, including direction on ensuring that online services provided by agencies are secure and protect privacy.
- NIST has developed standards and guidelines for implementing security controls, including those for authenticating users during online transactions.
- DHS has issued a directive requiring departments and agencies to mitigate critical vulnerabilities on their Internet-facing systems. It also assists agencies in monitoring their networks for malicious traffic.