

Auditors: IRS computers may be vulnerable to attack

Monday April 7, 1:56 pm ET

http://biz.yahoo.com/cnnm/080407/040708_irs_computers.html?.v=5&.pf=taxes

As taxpayers rush to file tax returns, independent auditors are warning that the Internal Revenue Service has not done enough to safeguard some of its computer systems, leaving sensitive taxpayer information vulnerable to disgruntled IRS employees, contractors or hackers.

Unscrupulous people could "reconfigure [computer] routers and switches" and "steal taxpayer information in a number of ways, including diverting information to unauthorized systems," according to the Treasury Inspector General for Tax Administration (TIGTA) office, which serves a watchdog function over the IRS.

The IRS says it has addressed the concerns raised in the report.

At issue is the security of routers and switches, devices that determine the proper path for data to travel between computer networks, TIGTA said. Because the IRS sends sensitive taxpayer and government information across its networks, it must have security controls to deter and detect unauthorized users.

The report does not indicate whether any taxpayer information has ever been misdirected or stolen from IRS computers, but said that in more than 84% of the 5.2 million times employees accessed a system to administer and configure routers, they used "accounts" that were not properly authorized.

To ensure security, the IRS had authorized 374 accounts for employees and contractors to use to access routers and switches to perform system administration duties, the TIGTA said. Of those, authorization for 86 had expired at the time of TIGTA's review in 2007, and there was no record that 55 employee and contractor accounts had ever been authorized.

"We are particularly concerned that 27 of the 55 employees and contractors had accessed the routers and switches to change security configurations," wrote Michael R. Phillips, the deputy inspector general who wrote the report.

In addition, nine accounts were still active, even though the employees and contractors had not accessed the system for more than 90 days, the report says. The IRS should have automatically prevented users from accessing routers and switches after 90 days, it says.

The report does not say whether anyone wrongly obtained taxpayer information or if taxpayer information was misused, but says it is continuing to review security to see whether changes made to the computer system were appropriate or warranted.

In a written response accompanying the report, the IRS said it has made some changes and is continuing to improve the control and monitoring of controls and switches. All 369 users now have current and valid authorizations on file, the IRS said.

-- from CNN Producer Mike M. Ahlers