

IRS Found Lax in Protecting Taxpayer Data

By Kathleen Day
Washington Post Staff Writer
Thursday, April 5, 2007; D01

Thousands of taxpayers could be at risk of identity theft or other financial fraud because the Internal Revenue Service has failed to adequately protect information on its 52,000 laptop computers and other storage systems, a new government report concludes.

The IRS did not begin to adequately correct the security problems until the second half of 2006, despite being warned about them in 2003 and again in February 2006, according to a report by the inspector general of the IRS, J. Russell George.

"If taxpayers don't feel their personal information is protected, that could make them less likely to voluntarily file their taxes," said assistant inspector general Margaret E. Begg, whose auditing office studied IRS security policies and practices in place from January 2003 through mid-June 2006.

Nearly 500 IRS laptops were lost or stolen during that 3 1/2 -year period, many from the homes or cars of IRS workers but a significant number -- 111 -- from IRS offices, the report found. The IRS says one laptop typically contains information on 10 to 25 tax cases.

Although the missing laptops could not be examined, the inspector general's staff tested 100 laptops currently used by IRS employees and found 44 had "unencrypted sensitive data, including taxpayer data and employee personnel data," leading investigators to conclude "it is very likely a large number of the lost or stolen IRS computers contained similar unencrypted data."

No report of identity theft has been linked to the missing laptops, and no taxpayers have been alerted to the potential security breaches, IRS officials say.

In previous reports in 2003 and 2006, the IRS inspector general's office found that agency employees often failed to encrypt information on laptops and that passwords and other access codes were often easy to bypass. The new report, released yesterday, found not only that the laptop problems persisted through much of 2006 but identified for the first time similar security holes in backup systems at IRS field and processing offices around the country.

In one instance, "an employee wrote user account names and passwords to the computer and various systems to which the employee has access on a piece of paper that was taped to the laptop," the report says.

The report attributes the newly identified shortcomings at IRS offices "to a lack of emphasis by management."

The security lapses described by the report are the latest instance of personal information being put at risk in recent years by a federal agency, even as identity theft has become one of the fastest-growing white-collar crimes. Last May, the Department of Veterans Affairs reported the theft of a computer hard-drive that contained personal information on more than 26 million people. A year ago, the Commerce Department reported that more than a thousand of its laptops were missing, including many containing sensitive information about individuals.

The government's missteps are mirrored in the private sector, where such companies as CardSystems Solutions and the owner of retail chains T.J. Maxx and Marshalls have had high-profile breaches of credit card information on millions of consumers. The Privacy Rights Clearinghouse, a nonprofit research and advocacy group in San Diego, says more than 100 million records of U.S. residents have been exposed by security breaches since February 2005.

Advertisement

MarketWatch
Mutual Fund/ETF Section
CLICK HERE
expert commentary
top analyst data
for our exclusive insight
video interviews

The inspector general's report said that in at least two instances the IRS said it had implemented recommendations from the 2003 and 2006 reports, including reminding employees to encrypt information and to reset security codes after laptops were serviced. But the new report says the inspector general's staff members "were unable to find any supporting documentation" that these remedies had been made and that, in any case, the IRS responses "have not been effective."

In an e-mailed statement, IRS Commissioner Mark W. Everson said the agency has had no reports of identity theft or other fraud resulting from the missing laptops but that mistakes were made that need correcting.

He said "protection of taxpayer data is a top priority" for the IRS and that the agency has "moved aggressively" since late summer to remedy security flaws. Historically, the agency treated missing laptops as lost hardware rather than as a possible loss of taxpayers' personal information.

"Clearly, this was not the proper response," he said.

An IRS spokesman said that since last fall, the agency's 100,000 employees have been trained in computer security, that nearly all laptops have been installed with automatic encryption software and that locks have been issued for all laptops.

Two powerful senators on the Senate Finance Committee, which oversees the IRS, said they are troubled by the report.

Committee Chairman Max Baucus (D-Mont.) said "sloppy security" can't be tolerated. The committee's ranking Republican, Charles E. Grassley of Iowa, agreed, saying "it's hard to see why this is still a problem when the IRS knew about it more than three years ago."

© 2007 The Washington Post Company