



## COMPUTERWORLD Security

 Print Article  Close Window

# Report: 490 IRS laptops lost or stolen over nearly three years

Linda Rosencrance

**April 05, 2007** (Computerworld) In nearly three years, 490 laptops were lost or stolen from the Internal Revenue Service, according to an [audit](#) by the Treasury Inspector General for Tax Administration.

Between Jan. 2, 2003, and June 13, 2006, a "large number" of the laptops were stolen from the vehicles and homes of IRS employees, while 111 were stolen from IRS facilities, according to the report released last month.

Although auditors were unable to determine what taxpayer information was contained on the missing laptops, they said employees are not adequately protecting taxpayers' personal information contained on IRS laptops.

"We conducted a separate test on 100 laptop computers currently in use by employees and determined 44 laptop computers contained unencrypted sensitive data, including taxpayer data and employee personnel data," the report said. "As a result, we believe it is very likely a large number of the lost or stolen IRS computers contained similar unencrypted data."

Auditors said IRS employees did not follow the department's encryption procedures because they were unaware of security requirements, did so for their own convenience or did not know the personal data was considered sensitive.

"We also found other computer devices, such as flash drives, CDs and DVDs, on which sensitive data were not always encrypted," according to the report. "We reported similar findings in July 2003, but the IRS had not taken adequate corrective actions."

Although the IRS also requires employees to restrict access to their laptops with usernames and passwords, 15 of the 44 laptops that contained unencrypted data also had security weaknesses that could be exploited to bypass these security controls, the auditors said.

"We believe system administrators either incorrectly configured the computers upon deployment or did not correctly reset the controls after working on the computers," the auditors said. "We also evaluated the security of backup data stored at four offsite facilities. Backup data were not encrypted and adequately protected at the four sites."



In a written response to the report, Richard Spires, CIO of the IRS, said his agency was taking aggressive steps to mitigate the risk of potential identity theft or other fraudulent activity, including providing IRS employees with the capability to encrypt sensitive files and e-mails on their computers; deploying full disk encryption technology and physical cable locks on all employee laptops; and identifying a secure encryption alternative for tapes exchanged with federal, state and other partners.

In a statement e-mailed to *Computerworld*, IRS Commissioner Mark Everson said protection of taxpayer data is a top priority of the IRS and the agency has moved aggressively in this area since this issue was raised a year ago.

"The IRS has vast amounts of taxpayer data. Our systems have extensive protection from outside penetration," he said in the statement. "There have been and continue to be numerous attempts to breach our firewalls, but none of these efforts has been successful."

Everson said the IRS is unaware of any identity theft cases stemming from the loss of laptops, but he conceded the report has correctly identified past shortfalls concerning the IRS laptops.

"These laptops, which typically have very limited data, had been routinely but not always encrypted," he said. "Historically, missing laptops were treated by us and [the Inspector General for Tax Administration] as a loss of IT hardware rather than as a potential loss of taxpayer data or personally identifiable information. Clearly, this was not the proper response."

Since last summer, the IRS has taken steps to address this issue, Everson said. For example, before a laptop is issued, it is encrypted, he said. All but about two dozen of more than 52,000 IRS laptops have been encrypted, he said.

"When a laptop is missing, the process now assesses the potential information affected as well as the hardware loss," he said. "We have emphasized employee training as well as focusing on reporting incidents and increased accountability."