

May 23-25, 2007 • Rosen Centre Hotel • Orlando, FL • [www.ispcon.com](http://www.ispcon.com)

## What's **HOT** in Internet Services

[www.internetnews.com/bus-news/article.php/3669971](http://www.internetnews.com/bus-news/article.php/3669971)

[Back to Article](#)

### IRS Audits Self Into Data-Theft Hot Seat

By [Roy Mark](#)

April 5, 2007

Taxpayers won't be the only ones explaining themselves to the government next week. So will the tax collectors.

U.S. Senator Chuck Grassley (R-Iowa) said Wednesday he plans to hold the Internal Revenue Service (IRS) accountable for its almost 500 missing or stolen laptops over the last three years during a Senate Finance Committee hearing next week. According to an IRS internal audit, many of the machines were likely holding unencrypted, sensitive taxpayer data.

"It's hard to see why this is still a problem when the IRS knew about it more than three years ago," Grassley said in a statement. "One stolen IRS laptop could put thousands of taxpayers in jeopardy. I plan to ask what the IRS is doing to fix this problem for good."

The audit, released this week, found "limited definitive information" on the number of taxpayers' affected. However, a separate test on 100 laptops currently in use by IRS employees determined 44 laptops contained unencrypted sensitive data on taxpayers and IRS employees. The audit also found other mobile computer devices, such as Flash drives with unencrypted data.

"We believe it is very likely a large number of the lost or stolen IRS computers contained similar unencrypted data," the audit states. "We reported similar findings in July 2003, but the IRS had not taken adequate corrective actions."

IRS Commissioner Mark W. Everson said in a statement the IRS is unaware of any identity-theft cases stemming from the loss of any laptops, but admitted the report correctly identified security shortfalls concerning the agency's laptops.

"The IRS is a field-based organization and our employees use laptops for day-to-day activity," Everson said. "These laptops, which typically have very limited data, had been routinely but not always encrypted."

Everson added that missing or stolen IRS laptops were historically treated as a loss of hardware and not a potential loss of taxpayer data and other personally identifiable information. "Clearly, this was not the proper response."

According to Everson, all but "roughly two dozen" IRS laptops have now been encrypted, and when a laptop is reported missing, "The process now assesses the potential information affected as well as the hardware loss."

In addition to lax encryption standards, the audit found the IRS struggling with usernames and passwords. Of the 44 unencrypted laptops tested, 15 had security weaknesses that could be exploited to bypass security access controls.

"We believe system administrators either incorrectly configured the computers upon deployment or did not correctly reset the controls after working on the computer."

The audit also revealed unencrypted backup data at four IRS off-site facilities. In one case, a non-IRS employee had full access to a storage area. In another example cited, envelopes and boxes with backup media were open and not resealed. "We attributed these weaknesses to a lack of emphasis by management," the audit states.

Everson said the IRS has emphasized employee training since last summer, as well as focusing on reporting incidents and increased accountability. "Protection of taxpayer data is a top priority of the IRS," he said. "The IRS has moved aggressively in this area since this issue was raised a year ago."

The audit comes more than three years after the General Accountability Office (GAO) [criticized](#) the agency's



handling of the data it collects from Americans. A year after that report, an internal audit [revealed](#) more than one-third of IRS employees and managers handed over sensitive login and password information to undercover agents posing as computer technicians.

The IRS laptop security problem is another in a series of embarrassing data leaks by government agencies.

Last May, the Veterans Administration (VA) [announced](#) approximately 26.5 million veterans were at risk of identity theft after a VA employee violated agency policy and took a laptop with the information on it home, where it was then stolen in a burglary. The incident was the second-largest data breach on record and the largest Social Security numbers breach ever.

The laptop was eventually [recovered](#), and an FBI forensics test indicated that no one compromised the personal data.

Data breach announcements at the [Navy](#), [Department of Agriculture](#) and the [Federal Trade Commission](#) soon followed.

-->

[Contact internetnews.com staff](#)

**JupiterWeb networks:**



Search JupiterWeb:

[Jupitermedia Corporation](#) has two divisions: [Jupiterimages](#) and [JupiterWeb](#)

[Jupitermedia Corporate Info](#)

Copyright 2007 Jupitermedia Corporation All Rights Reserved.  
[Legal Notices](#), [Licensing](#), [Reprints](#), & [Permissions](#), [Privacy Policy](#).

[Web Hosting](#) | [Newsletters](#) | [Tech Jobs](#) | [Shopping](#) | [E-mail Offers](#)

