



Text Size: A A A A

## Contractors Expose Taxpayer Data Associated Press

Story location: <http://www.wired.com/news/business/0,1367,64272,00.html>

*01:45 PM Jul. 19, 2004 PT*

Private contractors revamping IRS computers committed security violations that significantly increased the possibility that private taxpayer information might be disclosed, Treasury Department inspectors say.

An investigation by the department's [inspector general for tax administration](#) found that employees working for contractors, or an experienced hacker, could use the contractors' computers to gain access to taxpayer data.

"Our concerns were increased when we could not find documentation that all contractor employees had received background investigations as required," the report said.

Other lapses left the IRS computer system vulnerable to viruses and hackers, investigators said.

"In summary, a contractor's employees committed numerous security violations that placed IRS equipment and taxpayer data at risk," the report found. "In some cases, contractors blatantly circumvented IRS policies and procedures even when security personnel identified inappropriate practices."

In response, an IRS official acknowledged security problems but said the agency found no evidence to support contentions that there was a big risk that hackers could gain access to IRS computers or that taxpayer confidentiality would be breached.

"We can find no evidence of contractor activities that resulted in unrestricted access to production systems or taxpayer data," Daniel Galik, chief of IRS mission assurance, wrote to inspectors. "In the absence of documented incidents, we must conclude that much of your assessment is based on theoretical possibilities."

The report comes as Congress considers giving the IRS authority to hire private contractors to collect overdue tax debts, an effort that has some lawmakers and others worried that taxpayer information won't be protected.

"They obviously do not have good systems in place to monitor the contractors today," said Colleen Kelley, president of the National Treasury Employees Union. "This will result, for taxpayers, in very aggressive tactics by debt collectors."

The employees' union obtained a copy of the report through the Freedom of Information Act. Portions identifying the contractor, its employees and IRS personnel practices were not shown.

Treasury inspectors also found that after their auditors conducted the exam and the security violations became known, the IRS granted the contractor "root" access to the computer system. Root access gives a user permission to make unlimited and unrestricted changes to any part of the computer system, including the ability to turn off mechanisms that monitor users' actions.

The inspectors raised additional concerns:

- Unauthorized chat and instant-messaging activity left the IRS vulnerable to hackers who use those avenues to get information about an organization's internal computer architecture.
- Contractors' computers were vulnerable to hackers and viruses because they did not have security patches for known vulnerabilities in operating software.
- Some computers used by contractors were too old to support a secure operating system, and the IRS did not have enough money to replace them.

The inspector general reviewed four contracts last year in which contractors had access to critical equipment and systems. The IRS has over 900 contracts with private companies and consultants.



#### Ads by Google

|  |  |   |
|--|--|---|
| Contractors License<br>California Contractors<br>License Schools<br>www.contractorschool.com | Contractor License CA<br>contractors license exam<br>prep<br>100% pass practice exams<br>and bonds<br>www.contractorsbonds.com | Increase Your Roofing<br>Biz<br>Confirmed<br>Appointments<br>w/Qualified<br>Roof Buyers, Pay On<br>Sold Jobs!<br>www.Servicesmith.c |
|--|--|---|

---

**Wired News:** [Staff](#) | [Contact Us](#) | [Advertising](#) | [RSS](#) | [Blogs](#) | [Subscribe](#)  
We are translated daily into Spanish, Portuguese, and Japanese

© Copyright 2004, Lycos, Inc. All Rights Reserved.

Your use of this website constitutes acceptance of the Lycos **Privacy Policy** and **Terms & Conditions**