



Treasury Inspector General for Tax Administration

THE INTERNAL REVENUE SERVICE IS NOT ADEQUATELY PROTECTING TAXPAYER DATA ON LAPTOP COMPUTERS AND OTHER PORTABLE ELECTRONIC MEDIA DEVICES

Issued on March 23, 2007

Highlights

Highlights of Report Number: 2007-20-048 to the Internal Revenue Service Chief Information Officer and Chief, Mission Assurance and Security Services.

IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) annually processes more than 220 million tax returns containing personal financial information and personally identifiable information, such as Social Security Numbers. If lost or stolen, taxpayer data can be used to identify theft and/or other fraudulent purposes. The risk of loss is particularly high because IRS employees are allowed to take electronic taxpayer data outside of the office for business purposes and the IRS has over 47,000 portable laptop computers assigned to its employees.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of the Fiscal Year 2006 Annual Audit Plan and followed up on our findings from previous years that addressed noncompliance with procedures for safeguarding taxpayer data.

TIGTA conducted the review to determine whether the IRS is adequately protecting sensitive data on laptop computers and portable electronic media devices. The audit focused on identifying the number of lost laptop computers, determining whether data on those computers were encrypted, and determining whether laptop computer access controls were adequate. TIGTA also determined whether data on backup tapes stored at non-IRS offsite locations were encrypted and adequately secured.

WHAT TIGTA FOUND

IRS employees reported the loss or theft of at least 490 computers and other sensitive data in 387 separate incidents between January 2, 2003, and June 13, 2006. During this period, the IRS computer security organization was made aware of only 91 (24 percent) of the 387 incidents.

TIGTA determined 176 incidents likely did not involve any loss of taxpayer data, but 126 incidents involved the loss of personal information for at least 2,359 individuals. TIGTA was unable to determine the effect on taxpayers for 85 incidents due to a lack of details in the incident documentation.

A separate test of 100 laptop computers currently in use by employees determined 44 laptop computers contained unencrypted sensitive data, including taxpayer data and employee personnel data. In addition, 15 of the 44 laptop computers had incorrect settings that would allow anyone to bypass the password controls and access the contents on the laptop computer. Consequently, it is very likely that a large number of the lost or stolen IRS computers contained unencrypted data that could be easily accessed and read by persons gaining possession of the computers. Also, backup tapes were not encrypted and adequately protected at non-IRS offsite locations reviewed.

WHAT TIGTA RECOMMENDED

TIGTA recommended the Chief, Mission Assurance and Security Services, refine incident response procedures to ensure sufficient details are gathered regarding taxpayers potentially affected by a loss, periodically remind employees of their responsibilities for protecting computer devices along with the disciplinary actions for noncompliance of these responsibilities, and purchase cable locks as an extra layer of security for employees to protect their laptop computers.

TIGTA also recommended the Chief Information Officer include a reminder about encrypting sensitive information in the employees' annual certification of security awareness, consider implementing a systemic disk encryption solution on laptop computers that does not rely on employees' discretion for determining what data to encrypt, require system administrators to check security configurations when servicing computers, implement procedures to encrypt backup data sent to non-IRS offsite facilities, and conduct an annual inventory validation of backup media and a physical security check of the offsite facility used to store the media.

In their response to the report, IRS officials agreed with our findings and have taken or planned appropriate corrective actions to our recommendations. For two of the recommendations, the IRS offered alternative corrective actions that adequately addressed our findings. As such, TIGTA concurred with the planned corrective actions.

READ THE FULL REPORT

To view the report, including the scope, methodology, and full IRS response, go to:

<http://www.treas.gov/tigta/auditreports/2007reports/200720048fr.pdf>.

Email Address: Bonnie.Heald@tigta.treas.gov
Web Site: <http://www.tigta.gov>

Phone Number: 202-927-7037