



## Treasury Inspector General for Tax Administration Office of Audit

### **SIGNIFICANT IMPROVEMENTS HAVE BEEN MADE TO PROTECT SENSITIVE DATA ON LAPTOP COMPUTERS AND OTHER PORTABLE ELECTRONIC MEDIA DEVICES**

Issued on August 31, 2009

## Highlights

Highlights of Report Number: 2009-20-120 to the Internal Revenue Service Chief Technology Officer.

### **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. While the IRS has made significant improvements to protect sensitive data on laptop computers and other portable electronic media devices, controls over incident reporting and backup data require additional improvements. As a result, taxpayers may not be notified when security incidents involving their personal data have occurred and taxpayer data may be at risk of unauthorized disclosure.

### **WHY TIGTA DID THE AUDIT**

This review was included in TIGTA's Fiscal Year 2008 Annual Audit Plan as part of the statutory requirements to annually review the adequacy and security of IRS information technology. Since 2003, TIGTA has conducted at least three reviews that found internal control weaknesses in the IRS' safeguarding of taxpayer data on laptop computers and other portable electronic media. TIGTA conducted this review to follow up on a prior review and determine whether the IRS is adequately protecting sensitive data on laptop computers and other portable electronic media devices. TIGTA also evaluated the controls over incident reporting and backup data.

### **WHAT TIGTA FOUND**

The IRS has effectively implemented encryption technologies on laptop computers and other portable storage devices. These systemic encryption solutions have strengthened the protection of taxpayer data and personally identifiable information and have reduced the chance of unauthorized disclosure of sensitive data when laptop computers and other portable electronic media are lost or stolen.

However, TIGTA identified two areas where continued diligence is needed. First, IRS processes for tracking

*Email Address: [inquiries@tigta.treas.gov](mailto:inquiries@tigta.treas.gov)*

*Web Site: <http://www.tigta.gov>*

and sharing security incidents did not ensure that all affected organizations received and exchanged information related to all reported incidents in a timely manner. For example, TIGTA identified 85 incidents involving the loss of taxpayer data in hard copy format that were not shared by all affected organizations. As a result, the IRS did not review 22 of these incidents to determine whether taxpayers should be informed or offered assistance in protecting themselves from harm.

Second, the IRS did not always conduct annual inventory validations of backup data at offsite storage facilities as required or timely validate access lists of IRS employees authorized to access backup data at offsite facilities. As a result, TIGTA identified 15 individuals on an access list who no longer had a business need to have access to the backup data at the offsite facility. In addition, one headquarters office was not sending its backup data offsite to ensure its availability in the event of a disaster.

### **WHAT TIGTA RECOMMENDED**

TIGTA recommended that the Chief Technology Officer ensure that 1) the IRS collaborates with TIGTA to revise the Memorandum of Understanding to ensure all incidents involving personally identifiable information in electronic or hard copy form are properly reported and shared between the IRS Computer Security Incident Response Center and the TIGTA Office of Investigations, and 2) all backup data are properly protected from unauthorized access and disclosure.

In their response to the report, IRS officials agreed with the recommendations. The IRS Computer Security Incident Response Center plans to collaborate with the TIGTA Office of Investigations and other internal IRS organizations to revise the Memorandum of Understanding to better represent the current environment of incident reporting and sharing. In addition, the Enterprise Operations organization plans to initiate consolidation of media management into one organization to ensure consistency in media management and policy. The Modernization and Information Technology Services organization plans to ensure media management controls are in place to protect backup data from unauthorized access.

### **READ THE FULL REPORT**

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

<http://www.treas.gov/tigta/auditreports/2009reports/200920120fr.pdf>

*Phone Number: 202-622-6500*