



## Treasury Inspector General for Tax Administration

### **EFFORTS HAVE BEEN MADE, BUT MANAGER AND EMPLOYEE NONCOMPLIANCE WITH SECURITY POLICIES AND PROCEDURES PUTS PERSONALLY IDENTIFIABLE INFORMATION AT RISK**

Issued on August 13, 2007

## Highlights

Highlights of Report Number: 2007-20-117 to the Internal Revenue Service Chief Information Officer.

### **IMPACT ON TAXPAYERS**

The Internal Revenue Service (IRS) processes and maintains personally identifiable information for more than 130 million taxpayers who file their income tax returns with the IRS. While the IRS has accomplished several noteworthy actions to protect this information, managers and employees have not complied with established security procedures. As a result, personally identifiable information is being unnecessarily exposed to unauthorized access and potential identity theft.

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

This audit was initiated as part of a statute that requires each agency's Inspector General to review the policies and procedures related to personally identifiable information and conduct reviews at least every 2 years to ensure it is adequately protected. The overall objective of this review was to determine the progress the IRS has made in ensuring the security and privacy of personally identifiable information it maintains.

### **WHAT TIGTA FOUND**

The IRS has taken several noteworthy actions to protect taxpayer data in its possession. For example, it has established a Security Services and Privacy Executive Steering Committee to serve as the primary governance body for all matters relating to security and privacy issues in the IRS. In addition, it has made steady progress each year in complying with the requirements of the Federal Information Security Management Act.

However, TIGTA reviews during Fiscal Years 2003 to 2007 have identified persistent computer security weaknesses that jeopardize the security of personally identifiable information. TIGTA continues to find that employees are not aware of the security risks inherent in their positions. For example, TIGTA reviews found that employees did not sufficiently safeguard laptop

*Email Address:* [Bonnie.Heald@tigta.treas.gov](mailto:Bonnie.Heald@tigta.treas.gov)  
*Web Site:* <http://www.tigta.gov>

computers and did not encrypt data on the computers; were susceptible to social engineering techniques that hackers could use to gain access to their systems; and ignored IRS policies on the use of email, which increased security vulnerabilities.

Even employees with key security responsibilities continue to ignore standard security configurations, often for their own convenience. One TIGTA review found that managers provided employees access to systems and data the employees did not need and were not aware of the access capabilities of their employees. Other TIGTA reviews found that technical controls in modernized systems and the security infrastructure were inadequate. Although industry guidance recommends that security controls be designed into new systems early in the development process, security has not been at the forefront when new systems are developed in the IRS. Waiting until systems are implemented to address security controls will most likely cost significantly more than if security controls were considered during the development of the systems.

It is clear that some IRS executives are not holding managers and employees accountable for carrying out their responsibilities and for ensuring managers and employees are aware of the security risks associated with their positions. For the IRS to make greater strides in improving computer security and protecting personally identifiable information, managers and employees must be aware of the security risks inherent to their positions and consider security implications in their day-to-day activities. Executives must clearly communicate expectations that procedures will be followed and take appropriate actions when procedures are not followed.

### **WHAT TIGTA RECOMMENDED**

Because TIGTA had already made recommendations related to the aforementioned issues in prior audit reports, no additional recommendations were made. TIGTA will continue to monitor the IRS' overall strategy and ability to protect and secure personally identifiable information in future security-related reviews.

In their response to the report, IRS officials agreed that, while progress is being made, more needs to be done to ensure the privacy and security over personally identifiable information is a fundamental and top priority. The IRS plans to continue to update its systems, processes, and training so employees are aware of the steps they must take to prevent taxpayer information from being compromised.

### **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/200720117fr.pdf>.

*Phone Number:* 202-927-7037