



## Treasury Inspector General for Tax Administration Office of Audit

### TAXPAYER DATA USED AT CONTRACTOR FACILITIES MAY BE AT RISK FOR UNAUTHORIZED ACCESS OR DISCLOSURE

Issued on May 18, 2010

## Highlights

Highlights of Report Number: 2010-20-051 to the Internal Revenue Service Chief Technology Officer and the Chief, Agency-Wide Shared Services

### IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) provides its taxpayer data to contractors who store and process the data at their own facilities in support of the IRS' mission of tax administration. These data can contain personally identifiable information, such as tax return data and Social Security Numbers. The IRS did not have effective processes to identify all contractors with IRS taxpayer data that require annual security reviews by the IRS and did not ensure computer security weaknesses identified at contractor facilities during security reviews have been corrected. As a result, taxpayer data may be at risk for unauthorized access or disclosure.

### WHY TIGTA DID THE AUDIT

This audit was initiated as part of our statutory requirements to annually review the adequacy and security of IRS information technology. The overall objective of this review was to determine whether the IRS had effective controls in place to ensure IRS taxpayer data are protected at contractor facilities.

### WHAT TIGTA FOUND

Current processes were not effective at identifying all contractors who receive IRS taxpayer data and may be subject to required security reviews. The Infrastructure Security and Reviews (ISR) office of the IRS Modernization and Information Technology Services organization Cybersecurity function identified contractors that require reviews by submitting a data call request asking the IRS business organizations to identify their contractors that process, store, or house IRS taxpayer data. However, this process did not identify all contractors who have been provided such data. Without an effective process for identifying the contractors receiving IRS taxpayer data, the IRS cannot ensure that all contractors who receive such data are being reviewed for computer security control weaknesses. As a result, the IRS cannot ensure that taxpayer data are protected

at contractor facilities.

TIGTA also found that current processes were not followed to ensure weaknesses identified by the ISR teams at contractor facilities were timely corrected. Our review of eight contractors visited by the ISR office during Fiscal Year 2009 found that the ISR office identified security weaknesses at all eight contractor facilities. TIGTA requested Plan of Action and Milestones documents for tracking these security weaknesses; however, the IRS was unable to provide the Plan of Action and Milestones documents for seven of the eight contractors TIGTA reviewed. To illustrate the importance of monitoring security weaknesses at contractors' facilities, the ISR office identified 6 repeat weaknesses during its Fiscal Year 2008 reviews and 24 repeat weaknesses during its Fiscal Year 2009 reviews that were not corrected from the prior fiscal years' review. These weaknesses included access control, configuration management control, and system integrity control issues. Without adequate oversight to monitor and confirm that security weaknesses are corrected at contractor facilities, security weaknesses will persist and taxpayer data will remain at risk of unauthorized access and disclosure.

### WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief, Agency-Wide Shared Services, and the Chief Technology Officer, identify the information system that can serve as the primary source for identifying contractors requiring reviews. The Director, Procurement, and the Director, Office of Privacy and Information Protection, should ensure appropriate indicators are captured on each existing contract with a disclosure and privacy impact, validate whether the IRS business organization provided any IRS taxpayer data to these contractors, and provide the appropriate notification and guidance to the responsible IRS business organizations to execute annual security reviews of contractors when required.

In addition, the Associate Chief Information Officer, Cybersecurity, should validate correction of ISR office reported security weaknesses and recommend a process for reporting weaknesses that remain unmitigated to increase the accountability of the responsible parties for remediation of security weaknesses. In their response to the report, IRS management agreed with our recommendations and plans to take appropriate 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/2010reports/201020051fr.pdf>.

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

Phone Number: 202-622-6500