



## Treasury Inspector General for Tax Administration Office of Audit

### THE RETURN REVIEW PROGRAM ENHANCES THE IDENTIFICATION OF FRAUD; HOWEVER, SYSTEM SECURITY NEEDS IMPROVEMENT

Issued on July 2, 2015

## Highlights

Highlights of Report Number: 2015-20-060 to the Internal Revenue Service Chief Technology Officer.

### IMPACT ON TAXPAYERS

During Fiscal Year 2013, there were almost 146 million individual income tax returns filed. Individual income tax withholding and tax payments totaled more than \$1.5 trillion, and almost \$312.8 billion in refunds were issued. Undetected tax refund fraud, including identity theft, has a significant impact on tax administration. It has the potential to erode taxpayer confidence in our Nation's tax system and results in significant unintended Federal expenditures.

### WHY TIGTA DID THE AUDIT

Tax fraud is a major challenge for the IRS. In February 2009, the IRS chartered the initiation of a new program called the Return Review Program (RRP). The IRS plans to replace the Electronic Fraud Detection System with the RRP. Development of the RRP entered a strategic pause in January 2014 to allow the IRS time to evaluate the performance and design of the parallel processing database and to revisit strategic business fraud detection goals. Our overall objective was to determine if the RRP effectively meets requirements and identifies fraudulent tax returns.

### WHAT TIGTA FOUND

The RRP models flagged potential identity theft fraud not detected by the Electronic Fraud Detection System models. The IRS initiated a pilot of the RRP Identity Theft Model. Processing only 32 days (one day per week for 32 weeks) over the duration of the pilot, the RRP identified 51,946 returns as potential identity theft cases. The IRS confirmed that 41,311 of those returns were identity theft. Of the confirmed identity theft cases, the IRS determined that 10,348 cases (25 percent) totaling \$43 million in refunds were not detected by the Electronic Fraud Detection System or the Dependent Database. In addition, IRS tests showed that eight million returns a day can be loaded to the RRP database as required. For example, over a

one-week period, the RRP consistently loaded between seven million and nine million returns a day.

However, the IRS classified the RRP as a Level 3 system (an information resource instead of a major system). By classifying the RRP as a Level 3 Federal Information Security Management Act system, RRP-specific security issues may not be effectively addressed. In addition, identified security vulnerabilities were not remediated. For example, the October 2014 network scans identified two RRP servers that were still vulnerable to the Heartbleed bug six months after the vulnerability was announced.

### WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer: 1) ensure that IRS personnel completing the Federal Information Security Management Act system classifications are familiar with the Act's requirements; 2) ensure that the validation of system classification and reclassification is discussed, reviewed, and documented during the biweekly Cybersecurity management meeting; and 3) ensure that all critical and high-risk RRP vulnerabilities are resolved.

In their response to the report, IRS officials agreed with all three recommendations. The IRS plans to brief personnel on the Federal Information Security Management Act requirements for each level of classification; enhance its current process for the validation of system classification and reclassification as discussed, reviewed, and documented during the biweekly management meeting; and focus on resolving the critical vulnerabilities in production and then the lower environments.

### READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2015reports/201520060fr.pdf>