



Treasury Inspector General for Tax Administration Office of Audit

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION – FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT FOR FISCAL YEAR 2013

Issued on September 27, 2013

Highlights

Highlights of Report Number: 2013-20-128 to the Department of the Treasury, Office of the Inspector General, Assistant Inspector General for Audit.

IMPACT ON TAXPAYERS

The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. The Federal Information Security Management Act (FISMA) was enacted to strengthen the security of information and systems within Federal Government agencies. Until the IRS takes steps to fully implement all 11 security program areas covered by FISMA, taxpayer data will remain vulnerable to inappropriate use, modification, or disclosure, possibly without being detected.

WHY TIGTA DID THE AUDIT

As part of the FISMA legislation, the Offices of Inspectors General are required to perform an annual independent evaluation of each Federal agency's information security programs and practices. This report presents the results of TIGTA's FISMA evaluation of the IRS's information security program for Fiscal Year (FY) 2013.

WHAT TIGTA FOUND

Based on our FY 2013 FISMA evaluation, TIGTA found that nine of 11 security program areas were generally compliant with the FISMA requirements. Six of the nine security program areas included all of the program attributes specified by the Department of Homeland Security's (DHS) *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*:

- Continuous Monitoring Management.
- Risk Management.
- Plan of Action and Milestones.
- Contingency Planning.
- Contractor Systems.
- Security Capital Planning.

Three of the nine security program areas, while generally compliant, were not fully effective due to one program attribute that was missing or not working as intended:

- Incident Response and Reporting.
- Security Training.
- Remote Access Management.

However, two of the 11 security program areas were not compliant with FISMA requirements and did not meet the level of performance specified by the DHS's *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics* due to the majority of the DHS-specified attributes being missing or not working as intended:

- Configuration Management.
- Identity and Access Management.

WHAT TIGTA RECOMMENDED

TIGTA does not include recommendations as part of its annual FISMA evaluation and reports only on the level of performance achieved by the IRS using the guidelines issued by the DHS for the applicable FISMA evaluation period.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2013reports/201320128fr.pdf>