



Treasury Inspector General for Tax Administration Office of Audit

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION – FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT FOR FISCAL YEAR 2014

Issued on September 23, 2014

Highlights

Highlights of Report Number: 2014-20-090 to the Department of the Treasury, Office of the Inspector General, Assistant Inspector General for Audit.

IMPACT ON TAXPAYERS

The Federal Information Security Management Act of 2002 (FISMA) was enacted to strengthen the security of information and systems within Federal Government agencies. The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As custodians of taxpayer information, the IRS has an obligation to protect the confidentiality of this sensitive information against unauthorized access or loss.

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 for Fiscal Year 2014.

WHAT TIGTA FOUND

Based on this year's FISMA evaluation, five of the 11 security program areas met the performance metrics specified by the Department of Homeland Security's *Fiscal Year 2014 Inspector General Federal Information Security Management Act Reporting Metrics*:

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

Four security program areas were not fully effective due to one or more program attributes that were not met:

- Continuous Monitoring Management.
- Incident Response and Reporting.

- Security Training.
- Remote Access Management.

Two security program areas did not meet the level of performance specified due to the majority of the attributes not being met:

- Configuration Management.
- Identity and Access Management.

To meet the expected level of performance for Configuration Management, the IRS needs to improve enterprise-wide processes for assessing configuration settings and vulnerabilities through automated scanning, timely remediating scan result deviations, timely installing software patches, and controlling changes to hardware and software configurations.

To meet the expected level of performance for Identity and Access Management, the IRS needs to fully implement unique user identification and authentication that complies with Homeland Security Presidential Directive-12, ensure that users are only granted access based on needs, ensure that user accounts are terminated when no longer required, and control the improper use of shared accounts.

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 Department of Homeland Security 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/2014reports/201420090fr.pdf>.