



Treasury Inspector General for Tax Administration Office of Audit

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION – FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT FOR FISCAL YEAR 2011

Issued on September 20, 2011

Highlights

Highlights of Report Number: 2011-20-116 to the Department of the Treasury, Office of the Inspector General, Assistant Inspector General for Audit.

IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) collects and maintains a significant amount of personal and financial information on each taxpayer. The IRS also relies extensively on computerized systems to support its responsibilities in collecting taxes, processing tax returns, and enforcing the Federal tax laws. As custodians of taxpayer information, the IRS has an obligation to protect the confidentiality of this sensitive information against unauthorized access or loss. Otherwise, taxpayers could be exposed to invasion of privacy and financial loss or damage from identity theft or other financial crimes.

WHY TIGTA DID THE AUDIT

The Federal Information Security Management Act (FISMA) was enacted to strengthen the security of information and systems within Federal agencies. As part of this legislation, the Offices of Inspector General are required to perform an annual independent evaluation of each Federal agency's information security policies, procedures, as well as evaluate its compliance with FISMA requirements. This report reflects TIGTA's independent evaluation of the status of the IRS's information security program for Fiscal Year 2011.

WHAT TIGTA FOUND

Based on our Fiscal Year 2011 FISMA evaluation, TIGTA found the IRS's information security program was generally compliant with the FISMA legislation. Specifically, TIGTA determined that the following seven program areas met the level of performance specified by the Department of Homeland Security's Fiscal Year 2011 FISMA checklist.

- Risk management.
- Incident response and reporting.

- Remote access management.
- Continuous monitoring management.
- Contingency planning.
- Contractor systems.
- Security capital planning.

While the information security program was generally compliant with the FISMA legislation, the program was not fully effective as a result of the conditions identified in the following four areas:

- Configuration management.
- Security training.
- Plans of action and milestones.
- Identity and access management.

WHAT TIGTA RECOMMENDED

TIGTA does not include recommendations as part of our 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 Fiscal Year 2011 FISMA evaluation period.

READ THE FULL REPORT

To view the report, go to:

<http://www.treas.gov/tigta/auditreports/2011reports/201120116fr.pdf>.