



Treasury Inspector General for Tax Administration Office of Audit

Issued on November 10, 2010

Highlights

Highlights of Report Number: 2011-20-003 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 and procedures, as well as evaluate its compliance with FISMA requirements. This report reflects TIGTA's independent evaluation of the status of information technology security for unclassified systems at the IRS for Fiscal Year 2010.

WHAT TIGTA FOUND

Based on our Fiscal Year 2010 FISMA evaluation, TIGTA found the IRS's information security program was generally compliant with the FISMA legislation. Specifically, TIGTA determined that the following three program areas met the level of performance specified by the Office of Management and Budget's Fiscal Year 2010 FISMA checklist.

- Certification and accreditation program.
- Incident response and reporting program.
- Remote access management.

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 seven areas.

- Configuration management.
- Security training.
- Plans of action and milestones.
- Identity and access management.
- Continuous monitoring management.
- Contingency planning.
- Contractor systems/financial audit.

Specific to the financial audit area, the Government Accountability Office reported newly identified and unresolved information security control weaknesses in key financial and tax processing systems continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information. Until these control weaknesses are corrected, the IRS remains unnecessarily vulnerable to insider threats related to the unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as the disruption of system operations and services. These conditions were the basis for the Government Accountability Office's determination that the IRS had a material weakness in internal controls over financial reporting related to information security in Fiscal Year 2009.

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 Office of Management and Budget for the Fiscal Year 2010 FISMA period.

READ THE FULL REPORT

To view the report, go to:

<http://www.treas.gov/tigta/auditreports/2011reports/201120003fr.pdf>

Email Address: inquiries@tigta.treas.gov
Web Site: <http://www.tigta.gov>

Phone Number: 202-622-6500