



## Treasury Inspector General for Tax Administration Office of Audit

### TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION – FEDERAL INFORMATION SYSTEM MODERNIZATION ACT REPORT FOR FISCAL YEAR 2015

Issued on September 25, 2015

## Highlights

Highlights of Report Number: 2015-20-092 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, and its recent amendment, the Federal Information Security Modernization Act (FISMA) of 2014, were 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 this sensitive information against unauthorized access or loss in accordance with FISMA requirements.

### 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 2015.

### WHAT TIGTA FOUND

The IRS's Information Security Program generally complied with the FISMA requirements. Three program areas met all FISMA performance attributes specified by the Department of Homeland Security: *Risk Management, Incident Response and Reporting, and Contingency Planning*. Four other security program areas met all attributes with the exception of two or fewer program attributes that were not met: *Security Training, Plan of Action and Milestones, Remote Access Management, and Contractor Systems*.

However, three security program areas failed to meet FISMA requirements overall due to not meeting many of the performance attributes specified by the Department of Homeland Security: *Continuous Monitoring Management, Configuration Management, and Identity and Access Management*.

Until the IRS takes steps to improve its security program deficiencies and fully implement all security program areas in compliance with FISMA requirements, taxpayer data will remain vulnerable to inappropriate and undetected use, modification, or disclosure.

### WHAT TIGTA RECOMMENDED

TIGTA does not include recommendations as part of its annual FISMA evaluation and reports on only 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/2015reports/201520092fr.pdf>.