



Treasury Inspector General for Tax Administration Office of Audit

AUDIT TRAILS DID NOT COMPLY WITH STANDARDS OR FULLY SUPPORT INVESTIGATIONS OF UNAUTHORIZED DISCLOSURE OF TAXPAYER DATA

Issued on September 20, 2012

Highlights

Highlights of Report Number: 2012-20-099 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Audit trails are a key component of information technology security and contain a record of events occurring on a computer from system and application processes, as well as user activity. The IRS has taken actions to implement an enterprise solution to audit trail weaknesses, but incomplete audit trail data and inconsistent timestamps indicate audit trail processes need improvement. Insufficient audit trail data hinder investigations of unauthorized access (UNAX) to taxpayer information and IRS management's ability to enforce UNAX policies.

WHY TIGTA DID THE AUDIT

UNAX is prohibited by law. This audit was initiated to evaluate the IRS's efforts to implement effective UNAX audit trails for information systems that store and process taxpayer data. This audit is included in our Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

WHAT TIGTA FOUND

The Enterprise Security Audit Trail (ESAT) office has taken several actions to implement an enterprise solution to audit trail weaknesses. However, process improvements are needed to ensure audit trails effectively support UNAX investigations and IRS management's ability to identify noncompliant activity and hold employees accountable for UNAX policies.

Audit Plans, the key planning document to meet IRS goals to comply with audit trail standards, did not adequately identify all auditable events and related data elements that were required to be captured in the audit trail. Consequently, audit trail logs collected data as anticipated by Audit Plans but were still missing required data.

TIGTA observed application users while transactions were entered on three IRS applications that send audit trails to the Security Audit and Analysis System, the IRS's audit trail repository system. Multiple audit trail weaknesses were identified as a result of tracing these transactions. The IRS did not adequately validate audit log data that were sent to the Security Audit and Analysis System to ensure that the data necessary to support UNAX investigations are captured. The ESAT office did not conduct tests to determine if actions taken by users on the system correlated to events recorded in the audit trail log or if all required elements were being captured.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the ESAT office improves processes to ensure Audit Plans and resulting audit trails are accurate, complete, and compliant with requirements. In addition, processes to test audit trail data should be improved, and the Audit Plan template should be updated to identify the location of information on audit log testing and stakeholder comments and to show ESAT office approval that testing was sufficient. TIGTA also recommended that timestamp procedures be clarified and made readily available to application owners.

In their response, IRS officials stated they agreed with the recommendation to improve processes to test audit trail data. The IRS partially agreed with three recommendations. The IRS did not agree that validation should be completed before final ESAT office approval of Audit Plans, that Audit Plan templates should be updated to identify the location of information on audit log testing and stakeholder comments, or that guidance on timestamps needs revision, although they will review timestamp procedures.

TIGTA continues to recommend that the IRS formalize a location where test and ESAT validation results can be found, set shorter time frames to implement the proposed changes, postpone closing audit trail specific weaknesses, and revise timestamp procedures.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2012reports/201220099fr.pdf>