



Treasury Inspector General for Tax Administration Office of Audit

STRONGER ACCESS CONTROLS AND FURTHER SYSTEM ENHANCEMENTS ARE NEEDED TO EFFECTIVELY SUPPORT THE PRIVACY IMPACT ASSESSMENT PROGRAM

Issued on September 1, 2015

Highlights

Highlights of Report Number: 2015-20-079 to the Internal Revenue Service Director, Privacy, Governmental Liaison, and Disclosure.

IMPACT ON TAXPAYERS

A Privacy and Civil Liberties Impact Assessment (PCLIA) is a process for examining the risks and ramifications of using information technology to collect, maintain, and disseminate information in identifiable form, such as Social Security Numbers, about members of the public and agency employees. Among the most basic of taxpayers' and employees' rights is an expectation that the IRS will protect the confidentiality of personal, financial, and employment information.

WHY TIGTA DID THE AUDIT

This audit was initiated because the Consolidated Appropriations Act of 2005, Section 522, requires the Inspector General to evaluate the agency's use of information in identifiable form and the privacy and data protection procedures every two years. The overall objective of this review was to determine whether the Privacy Impact Assessment Management System (PIAMS) is effectively working as intended to support the privacy impact assessment program and is secure against unauthorized access.

WHAT TIGTA FOUND

The Privacy, Governmental Liaison, and Disclosure (PGLD) organization's Privacy Compliance and Assurance office has responsibility for oversight of the PCLIA process. To comply with applicable laws and regulations governing privacy, the IRS requires system owners to submit all new PCLIA's through the PIAMS. The PGLD organization fully implemented five of the nine recommendations made to address the weaknesses reported in the Fiscal Year 2013 review and implemented suggested user modifications to the PIAMS to effectively support the IRS's privacy impact assessment program. However, PIAMS access control improvements and additional system enhancements are needed. During our audit, TIGTA determined that the

Privacy Compliance and Assurance office was unable to provide authorizations supporting access to the PIAMS for 27 of 29 users with elevated privileges and changed the user roles and account statuses for 10 of the 29 users on the PIAMS. In addition, after TIGTA brought it to the PGLD organization's attention, it removed 12 of 41 users' accesses to its shared drive because they no longer had a business need.

During our independent testing, which included creating a fictitious PCLIA in a simulated process, TIGTA identified enhancements that could improve the assessment process. The enhancements included requiring a negative response when no sensitive information is identified in the PCLIA prior to the disclosure review for redaction.

WHAT TIGTA RECOMMENDED

TIGTA made six recommendations, including that the Director, PGLD, issue a communication to PGLD organization managers and employees reminding them to review user accounts for compliance with account management requirements and change the planned corrective action status from closed to open for corrective actions TIGTA identified as not fully implemented.

In their response, IRS management agreed with four of our six recommendations. The IRS disagreed with requiring system owners to provide a negative response when they review the assessment for sensitive information and with reopening planned corrective actions that were not fully implemented. TIGTA believes the negative responses are needed to provide assurance that requirements were received and understood, and that prematurely closed corrective actions should be reopened until fully completed to be consistent with Federal requirements.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2015reports/201520079fr.pdf>.

E-mail Address: TIGTACommunications@tigta.treas.gov

Phone Number: 202-622-6500

Website: <http://www.treasury.gov/tigta>