



Treasury Inspector General for Tax Administration Office of Audit

USING SMARTID CARDS TO ACCESS COMPUTER SYSTEMS IS TAKING LONGER THAN EXPECTED

Final Report issued on September 28, 2012

Highlights

Highlights of Report Number: 2012-20-115 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The President's Cyberspace Policy emphasized that agencies need to use SmartID cards to access computer systems. The IRS's efforts to upgrade its systems to use the SmartID cards are taking longer than expected. Upgrading the security of computer systems is important to prevent disruptions in critical IRS processes and to protect taxpayers' personal information from unauthorized access.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the implementation and security of the IRS's two-factor authentication system for accessing computer systems. Two-factor authentication is a secure approach to verifying employees' identities on a system and requires the presentation of two identifying factors: something the user knows (a personal identification number) and something the user has (a SmartID card). Two-factor authentication provides significant improvement in computer security in terms of allowing access to systems.

WHAT TIGTA FOUND

The IRS developed a two-factor authentication system with the required components. However, significant delays prevented the IRS from deploying the new two-factor authentication system as originally planned. The IRS originally planned to complete the deployment by September 2011. The deployment is now planned to be completed by July 2013.

In addition, the IRS did not appoint a project manager with the requisite training and experience to lead the Internal Identity and Access Management project, which included the two-factor authentication component. This decision led to numerous issues. The project team did not make adequate progress in some crucial areas such as: 1) developing two-factor authentication for computer administrators, 2) conducting required testing, and 3) completing key documents and processes.

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

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

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer direct IRS Labor Relations to notify the National Treasury Employees Union and begin negotiating mandatory use of the SmartID cards. TIGTA also recommended that the Assistant Chief Information Officer, Cybersecurity, appoint a certified project manager with the requisite training and experience to lead the Internal Identity and Access Management project and direct the project manager to ensure the required security control assessment is completed, select a method to implement two-factor authentication for administrators, coordinate the activities to ensure all required testing is completed, and complete the required documents and processes that are needed to fully test and evaluate the system.

The IRS agreed with seven of the recommendations and plans to bargain with the National Treasury Employees Union as appropriate on mandatory use of the SmartID Cards, appoint a certified project manager and provide adequate resources to the project, and assign project resources to determine if a viable solution for administrators' use of SmartID cards exists. The IRS disagreed with two recommendations regarding the completion of required testing of the new system and stated that testing was completed in accordance with its procedures and additional testing is not necessary.

TIGTA remains concerned about the IRS's disagreement on the issue of testing. The IRS did not conduct the required testing for the most significant part of the two-factor authentication system, which is the part employees will use to authenticate to the IRS network. TIGTA found no evidence that the security, integration, capacity, and performance testing were conducted for this crucial part of the system.

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/201220115fr.pdf>.

Phone Number: 202-622-6500