



Treasury Inspector General for Tax Administration Office of Audit

CONTINUED CENTRALIZATION OF THE WINDOWS ENVIRONMENT WOULD IMPROVE ADMINISTRATION AND SECURITY EFFICIENCIES

Issued on September 23, 2011

Highlights

Highlights of Report Number: 2011-20-111 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) operates a large computer network that includes about 6,000 servers and 110,000 workstations using Windows operating systems provided by the Microsoft Corporation. Proper implementation of Microsoft Corporation Windows technology simplifies system administration and provides methods to strengthen and consistently secure computer systems. When IRS operations run efficiently and securely, taxpayer dollars and data are preserved and protected.

WHY TIGTA DID THE AUDIT

This audit is included in our Fiscal Year 2011 Annual Audit Plan and addresses the major management challenge of Security. The overall objective of this review was to determine whether the IRS has structured its Windows environment to provide efficient and secure management of Windows servers.

WHAT TIGTA FOUND

The IRS has not taken actions to continue enforcing the centralization of its Windows environment, which would simplify system administration and achieve consistent identity and authentication management that is required by Federal regulations and IRS enterprise architecture security principles. TIGTA found three organizations that maintained groups of Windows servers outside of the main centralized group of Windows servers. The IRS spent \$1.2 million in contract fees to maintain obsolete computer equipment in one of these groups, rather than spending those funds to resolve the vulnerability.

In addition, the IRS did not ensure that all Windows computers connected to its network were authorized and compliant with security policy, putting the IRS at risk of security breaches. While the IRS had created standards to prevent unauthorized computers from being connected to the network, it had not established a

central controlling authority to enforce compliance with its policy.

WHAT TIGTA RECOMMENDED

The Chief Technology Officer should ensure that:

- 1) an enterprise-wide Active Directory governing body is established to enforce Windows server group design criteria and ensure unauthorized Windows server groups are not created;
- 2) planned shutdown of the noncentralized groups of Windows servers is continued or feasibility studies to collapse noncentralized Windows server groups are completed;
- 3) standards to prevent computers from being connected to the network without proper authorization and required compliance documentation are implemented enterprise-wide; and
- 4) network scanning tools are utilized to locate unauthorized computers on the IRS network, and adequate procedures are developed and implemented to ensure they are removed.

In its response to the report, the IRS agreed with TIGTA's recommendations and plans to take appropriate corrective actions. However, the IRS disagreed with TIGTA's \$1.2 million outcome measure related to the maintenance of obsolete computer equipment. TIGTA maintains the appropriateness of the measure.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2011reports/201120111fr.pdf>