



## Treasury Inspector General for Tax Administration Office of Audit

### AN ENTERPRISE APPROACH IS NEEDED TO ADDRESS THE SECURITY RISK OF UNPATCHED COMPUTERS

Issued on September 25, 2012

## Highlights

Highlights of Report Number: 2012-20-112 to the Internal Revenue Service Chief Technology Officer.

### IMPACT ON TAXPAYERS

Patch management is an important element in mitigating the security risks associated with known vulnerabilities. The IRS has taken some actions to address patch management weaknesses, but an enterprise approach is needed to fully implement and enforce patch management policy. Any significant delays in patching software with critical vulnerabilities provides ample opportunity for persistent attackers to gain control over the vulnerable computers and get access to the sensitive data they may contain, including taxpayer data.

### WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the effectiveness of the IRS security patch management process. The implementation of effective patch management processes has been an ongoing challenge for the IRS, with patch issues reported in numerous prior TIGTA and Government Accountability Office reports. 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

Although progress has been made to automate installation and monitoring of patching in a large segment of its Windows environment, the IRS has not yet implemented key patch management policies and procedures needed to ensure all IRS systems are patched timely and operating securely. Specifically, the IRS has not completed implementation of an accurate and complete inventory of its information technology assets, which is critical for ensuring that patches are identified and applied timely for all types of operating systems and software used within its environment.

In addition, the IRS needs to improve patch policy and monitoring processes to ensure patches are applied timely. The IRS also has not implemented controls to ensure that unsupported operating systems are not putting the IRS at risk. The IRS needs enterprise-level

oversight and leadership to complete the implementation of its standardized patch management program and to achieve the benefits of implementing enterprise-wide patching solutions.

### WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS implement enterprise-level responsibility to set and enforce IRS patch management policy, complete deployment of an automated asset discovery tool and build an accurate and complete inventory of information technology assets, take an enterprise-wide approach to buying tools to avoid redundancy and excessive cost, and complete implementation of controls to ensure that unsupported operating systems are not putting the IRS at risk.

The IRS agreed with TIGTA's recommendations and planned appropriate corrective actions for seven of the eight recommendations. Although the IRS agreed with the intent of the recommendation to hold system owners accountable for patching computers within prescribed time frames, it stated that its existing procedures addressed this recommendation and planned no corrective actions. While TIGTA believes further actions could have been taken, TIGTA also believes the IRS will address this issue through other planned corrective actions to update its patch management policy to provide clear standards for patch installation and to assign the responsibility to the Cybersecurity organization for ensuring enterprise-wide compliance with patch management policies.

### 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/201220112fr.pdf>

E-mail Address: [TIGTACommunications@tigta.treas.gov](mailto:TIGTACommunications@tigta.treas.gov)

Phone Number: 202-622-6500

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