IRS Office of Safeguards Automated Testing Enhancements

December 31, 2016

What Is Changing?

As of September 2014, the Office of Safeguards will discontinue use of the ThreatGuard Secutor Prime compliance scanning tool that has been used to conduct compliance scanning on Windows platforms. In its place, we will employ Tenable Nessus, a tool with a well-established presence in the IT security world. The tool provides a scanning capability that will deliver enhanced information regarding the security controls in place to protect Federal Tax Information (FTI).

Why Are We Making the Change?

With the ever-increasing scope of Safeguard reviews, the Office of Safeguards requires a testing tool that provides comprehensive automation of compliance testing, and will scale with the continued increase in platform technologies that are used by agencies to store, process, transmit and/or receive FTI. Additionally, we operate in a complex threat environment that requires increased diligence and proactive risk management from all stakeholders to ensure the continued protection of FTI.

What Are The Benefits?

Nessus provides for increased automation of the compliance testing currently performed manually by the Safeguards Review Team. While maintaining the current compliance testing capability, the use of Nessus allows for the compliance testing of additional platforms (e.g., *NIX systems, network devices, etc.) to be automated, beyond the current capability for only Windows platforms.

By automating a greater portion of the review, the hours of support currently required of your system and network administrators for data collection will be greatly reduced, minimizing the disruption of normal business activities. Additionally, the agency will be provided enhanced information regarding security controls to support knowledge of security posture and improvement of the Safeguards program.

How Will Safeguard Reviews Be Different Using the Nessus Tool?

Compliance testing will continue to evaluate system security configurations for devices that store, process, transmit and/or receive FTI as is done today. However, automated testing will be performed on the majority of system platform types, as opposed to today which is limited to Windows devices.

There are some technical changes that will occur with the new testing, including conducting the testing from dedicated IRS testing hardware and coordination with agency technical staff for executing testing. Safeguards testing staff will work with agency staff in the months preceding the on-site review to ensure technical requirements are met prior to arriving on site. Additional information regarding technical details will be provided in the coming months as the deployment progresses.

What Will Not Be Changing?

The change in methodology will not have a discernible impact on how the results of reviews are reported. Agencies should expect initial, high-level information reported at the conclusion of the review through the Preliminary Findings Report (PFR), with more detailed findings and recommendations provided through the Safeguard Review Report.

Also, agencies will continue be provided access to the security configuration benchmarks used by the Safeguard Review Team to assess the security posture of systems that store, process, transmit and/or receive FTI and compliance with IRS security requirements.

What's Next and What If I Have a Question?
As planning for the deployment of the Nessus tool continues, please look for additional communications regarding technical details of the implementation of the tool for Safeguard reviews.

For questions or additional information, please contact the Office of Safeguards at SafeguardReports@irs.gov, or join during the monthly office hours for discussion of the tool and to submit questions to available technical staff.