



ISS Statement regarding Common Criteria practice

Submitted to the House Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census

by

Chris Klaus, Founder and CTO, Internet Security Systems, Inc.

The overall goal and intent of Common Criteria and NIAP certification of helping the government select the proper levels of security products is good, but the actual process and mechanics fail in its mission to properly evaluate and assess the robustness of security products. It fails in three major ways: accuracy, speed, and cost.

Accuracy: The current different levels of evaluation do not reflect whether the security product is actually more accurate in protecting against vulnerabilities and exposures. A government agency could falsely believe they have better protection with a higher level of certified products, but in reality, have less robust and accurate security products.

Speed: The current evaluation process is extremely bureaucratic and slow. It can take over a year before a product becomes certified. By the time a product becomes certified, it is outdated and behind the latest version of protection. The commercial sector could apply the latest version, while the government would lag behind in security. In the race against the cyber-crime threats, all organizations need to apply current security protection products.

Cost: The current evaluation process is extremely burdensome and costly for the security vendor to follow, and after following the process, the expense does not result in any security improvements in the products for the government. The resources and financial capital is better spent on making more robust and accurate security products. The evaluation process should reflect these improvements.

Because the current evaluation process fails in these three major areas, the government will actually become less secure if it follows the Common Criteria guidelines. The criteria and certification process needs to be dramatically revamped and overhauled with much stronger participation and input between government and the commercial sector for the certification process to improve.