Evaluating Commercial IT Products

FOR NATIONAL SECURITY SYSTEMS

With cyber threats growing exponentially, it's more important than ever for the U.S. military and federal government to acquire information technology products with the best possible balance of features, security and affordability. New commercial technologies offer advancements in computing, networking, mobility, and other areas that increase productivity and effectiveness. At the same time, agency budgets are under pressure, making procurement decisions even more complex than before. Fortunately there is a way military and federal leaders, acquisition officials, program managers, and users can take advantage of existing and emerging commercial IT products with the required level of cybersecurity.

How to Participate

Technical communities and working groups in many areas of technology have been formed and will be standing up in the months ahead – with opportunities for representatives from government agencies and industry to contribute to the development, maintenance and update of Protection Profiles. Additionally, the Common Criteria Users Forum offers a means to get involved with the international community of Common Criteria testing labs, industry, and government agencies globally.

For more information, please contact NIAP by email to niap@niap-ccevs.org or find us on the web at niap-ccevs.org.

N I A P

9800 SAVAGE ROAD
SUITE 6940
FT. MEADE, MD 20775-6940

Common Criteria

IT SECURITY EVALUATION

N I A P

NATIONAL INFORMATION ASSURANCE PARTNERSHIP

COTS + Common Criteria Testing = Unique Value

This value proposition for military and government IT security is based on Common Criteria testing of commercial off-the-shelf (COTS) products developed by U.S. and international vendors. Through the Common Criteria Recognition Arrangement (CCRA), 31 nations use the Common Criteria standard. In the U.S., the National Information Assurance Partnership (NIAP) oversees Common Criteria evaluations conducted under the CCRA. NIAP works in partnership with federal government customers, commercial IT vendors, certified independent testing labs, the National Institute of Standards and Technology (NIST), and other government agencies to ensure products meet the security requirements of customers. Under the process prescribed by the CCRA and NIAP for the U.S., vendors submit their products to accredited commercial labs for evaluation against technology-specific security requirements. Upon successful completion of the evaluation, they receive a Common Criteria certificate and are posted on the NIAP and the International Common Criteria evaluated products lists – approved for acquisition by the Defense Department, Department of Homeland Security, State Department, and other federal government users of National Security Systems.

This pathway satisfies Policy No. 11 of the U.S. Committee on National Security Systems (CNSS). As revised June 10, 2013, CNSS Policy 11 states that layered COTS product solutions of two or more evaluated IA and IA-enabled IT products "are preferred for use to protect information on NSS when these solutions are available and satisfy an organization's requirements." Compared to government-developed (GOTS) products, these certified commercial products typically will be lower in cost and available in a more timely fashion to meet evolving needs and to counter cyber threats. CNSS Policy 11 goes on to mandate, "All COTS IA and IA-enabled IT products acquired for use to protect information on NSS (National Security Systems) shall comply with the requirements of the NIAP program in accordance with NSA-approved processes and, where applicable, the requirements of the Federal Information Processing Standard (FIPS) Cryptographic validation program(s)."

Benefits for Customers and End Users

Under CNSS Policy 11, NIAP administers the U.S. Common Criteria Evaluation and Validation Scheme (CCEVS) – overseeing Protection Profile-based testing of products as a collaborative pathway for military and federal acquisition officials and program managers to identify needs and priorities, and to acquire commercial products without the need for future testing (and associated costs and delays) at the agency level. The Common Criteria route enables more precision in evaluations, greater clarity in acquisition decisions, a better balance of features, security and affordability, and more rapid access to commercially available products.

Benefits for Industry Partners

NIAP CCEVS offers value to the IT industry vendors too. The new Protection Profile-based approach to testing means more predictability, greater speed, less cost, and a wider U.S. and international market for evaluated products and emerging technologies. Through the CCRA, 31 nations mutually recognize Common Criteria evaluated products. In many cases, a vendor can have a product evaluated once and then sell it globally. The CCRA also serves end users who can purchase international products with greater confidence.

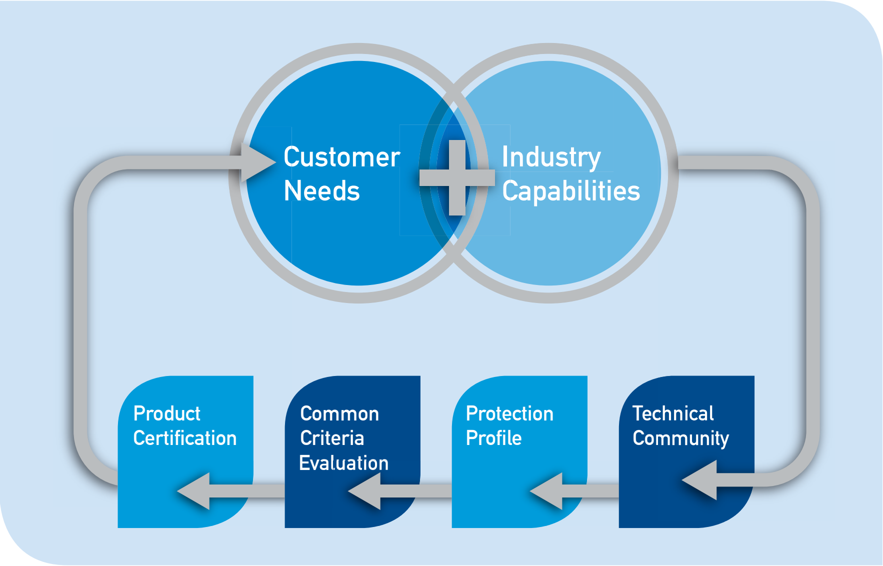
The Common Criteria Ecosystem

NIAP collaborates with a network of stakeholders that combines the perspectives and priorities of customers and vendors with international government partners, consultants, testing lab leaders, and academic experts:

CUSTOMERS: Military, intelligence community and other federal government officials and users of U.S. National Security Systems – plus their counterparts in other CCRA nations. They specify security functional and test requirements through the use of protection profiles.

VENDORS: U.S. and international producers who want to access the market of the U.S. and other governments with tested and approved IT products. Approved products have an even wider market in critical infrastructure and other private sector organizations, where Common Criteria testing is not required but is recognized.

TECHNICAL COMMUNITIES AND WORKING GROUPS: These are lively collaborations of representatives from military and government organizations along with product developers, integrators, testing labs, and consultants. Typically there is multinational representation. Together they focus on development of security and test requirements for specific technology areas such as mobility. The best approaches require the input of all the stakeholders involved; this is where synergy happens. Military and government agencies along with vendors, academia and labs define sets of specific security functional and test requirements they expect COTS products to meet. Then they work through technical communities to develop, maintain and update the Protection Profiles that serve as the specifications for efficient and effective Common Criteria evaluations.



TESTING LABS: These independent facilities conduct testing to ensure products meet vendors' claims about product security attributes according to the Common Criteria Protection Profiles. Labs must comply with standards set forth by the government bodies of certificate authorizing nations. They work in tandem with vendors.

SUBJECT MATTER EXPERTS: Consultants from industry, think tanks, and academic institutions contribute specialized expertise in the form of research, education, training, and guidance.

COMMON CRITERIA: Also known as international standards ISO/IEC 15408 and ISO/IEC 18045, Common Criteria is the driving force for the widest available mutual recognition of secure IT products. The recent shift to Protection Profile-based evaluations has enhanced the program further.

COMMON CRITERIA RECOGNITION ARRANGEMENT: 31 nations, including the U.S., agreeing to accept Common Criteria testing to improve the availability of evaluated, security-enhanced IT products and Protection Profiles; ensure evaluations are performed to consistent standards, and eliminate the burden of duplicating evaluations. Government, vendor, lab, and academic representatives from CCRA nations often work together in international technical communities.

COMMON CRITERIA USERS FORUM: A platform for all of those connected to Common Criteria to have a voice. With global industry participation, CCUF works to improve communication amongst consultants, labs, organization committees, government, and other interested parties.