Common Criteria IT Security Evaluation
& the National Information Assurance Partnership

The international Common Criteria Recognition Arrangement (CCRA) brings together 26 nations who agree to accept a unified approach to the evaluations of information technology products and protection profiles for information assurance and security. This arrangement benefits member nation governments and other customers of IT products by creating more clarity in procurement decisions, more precision in evaluations, a better balance of security and features, and more rapid access to products from industry.

For producers, Common Criteria in conjunction with the CCRA offers more predictable and timely evaluations at less cost – plus a wider international market for emerging technologies and products. Producers, customers and technical experts collaborate through international technical communities to develop, maintain and update the protection profiles that serve as the foundation for efficient and effective evaluations.

As the basis for the international standards ISO/IEC 15408 and ISO/IEC 18045, Common Criteria is a framework in which:

- government, military and other users can *specify* their security *functional* and *assurance* requirements through the use of protection profiles,
- vendors can then *implement* and/or make claims about the security attributes of their products,
- and testing laboratories can *evaluate* the products to determine if they actually meet the claims.

This framework provides assurance that the Common Criteria process of specification, implementation and evaluation of IT products has been conducted in a rigorous, standard, achievable, repeatable and testable manner at a level that is commensurate with the target environment for use.

The original Common Criteria was produced by unifying three pre-existing standards:

- **ITSEC** – The European standard, developed in the early 1990s by France, Germany, the Netherlands and the UK.
- **CTCPEC** – The Canadian standard followed from the US DoD standard.
- **TCSEC** – The United States Department of Defense DoD 5200.28 Std, called the Orange Book and parts of the Rainbow Series.

Originally developed by the governments of Canada, France, Germany, the Netherlands, the U.K., and the U.S, later versions of the Common Criteria were developed with significant contributions from other members of the CCRA.

Currently 26 nations recognize the Common Criteria and all are signatories to the Common Criteria Recognition Arrangement. This ensures that certificates of products evaluated using the Common Criteria are mutually recognized as meeting the standard. These certificates are recognized by all 26 nations, while 16 nations are certificate-producing

nations (as of August 2013). These 16 have programs in place to evaluate IT products using Common Criteria.

In the U.S., the National Information Assurance Partnership (NIAP) – a partnership between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) – is responsible for U.S. implementation of the Common Criteria, including management of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) validation body. CCEVS manages a national program for developing protection profiles, evaluation methodologies, and policies that will ensure achievable, repeatable, and testable requirements. In partnership with NIST, NIAP also approves Common Criteria Testing Laboratories to conduct these security evaluations in private-sector operations across the U.S.

NIAP takes a collaborative approach to technology-specific protection profile development by supporting the creation of international technical communities of representatives from industry, government, end users, and academia. This results in consistent evaluation methodologies across U.S. testing labs and among labs associated with international Common Criteria Recognition Arrangement schemes. Today's protection profiles take into account the current assurances achievable for specific commercial off-the-shelf (COTS) technologies. Assurance activities are developed to ensure consistent, obtainable results and to provide concise testing requirements that enable expeditious evaluations.

NIAP also works with NATO and international standards bodies (ISO) to share Common Criteria evaluation experiences and avoid duplication of effort. In the U.S., NIAP engages with other National Security Systems users to ensure protection profiles align with corresponding security documents including Security Requirements Guides/Security Technical Implementation Guides (SRGs/STIGs). The authority for NIAP to apply Common Criteria for security evaluations comes through the following policies:

- National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems"
- CNSS Policy (CNSSP) 11 "National Policy Governing the Acquisition of Information Assurance and IA-Enabled Information Technology Products"
- CNSS Directive (CNSSD) 502, "National Directive on Security of National Security Systems"
- Department of Defense Directives:
  - DoDD 5100.2, "National Security Agency/ Central Security Service"
  - DoDD 8500.01E, "Information Assurance"
  - DoDI 8500.02, "Information Assurance Implementation"

Currently NIAP has a suite of 18 published protection profiles and is managing development activities of 13 more profiles for technologies including Mobility and Virtualization – as well as updates to existing protection profiles for Intrusion Prevention System, Peripheral Sharing Switch, and others.

Collectively NIAP and the CCRA international members have certified over 2,100 commercial products. NIAP alone has managed the certification of over 460 evaluations.

Please visit our websites for the latest information:

NIAP®

niap-ccevs.org

Common Criteria®

commoncriteriaportal.org