# Executive Summary

Stakeholders in government and critical infrastructure sectors around the globe are increasingly looking for certified Information and Communication Technology (ICT) products that will meet their security needs.

At the same time, for security evaluations to demonstrate ICT products can effectively mitigate today’s top cyber security threats, an open community-based approach with all international participants recognizing Common Criteria is needed.

For over 15 years Common Criteria (CC) has been the leading international security certification standard for acquirers looking for validated security features of ICT products. Since its development by the governments of Canada, France, Germany, the Netherlands, the United Kingdom, and the United States, the number of participant nations has quadrupled and continues to increase –a resounding indicator to both the need and dependence on CC worldwide.

This paper introduces Common Criteria and provides insight into the revised Common Criteria Recognition Arrangement (CCRA). The revised CCRA will focus CC away from Evaluation Assurance Levels (EALs) to recognize collaborative Protection Profiles (cPPs) written by international Technical Communities (iTCs) ensuring certified products reach a worldwide common and accepted level of security assurance.

## Common Criteria – Introduction

The Common Criteria is a multi-part international standard for expressing security requirements along with common assurances and methodology for determining that the claimed functionality of an ICT product is sufficient to meet its security objectives. Conceptually it is a framework where:

* Vendors make security claims about their ICT product.
* Certified testing laboratories/facilities evaluate the ICT product to determine if the vendor’s implementation actually meets the security claims.
* End-users look for evaluation results that match their requirements – typically in the procurement process.

### Key Terms and Concepts

A *Protection Profile (PP)* expresses an implementation-independent set of security objectives for a type or category of ICT product. It also specifies the security requirements and assurance measures which fulfill those objectives.

A *Security Target (ST)* expresses security objectives of a specific ICT product and defines the functional requirements and assurance measures to fulfill those stated objectives. It also defines an implementation of the security requirements. The ST forms the basis for an evaluation and may claim conformance to one or more PPs.

The *CC standard documentation* set is identified and briefly described below:

* CC standard Part 1 provides an introduction and background to the CC model.
* CC standard Part 2 presents security requirements in distinct categories of behavior.
* CC standard Part 3 presents assurance requirements which are the basis for gaining confidence the claimed security measures are effective and are implemented correctly.
* Lastly, a common methodology for evaluation processes and evaluation tasks is provided in the CEM document.

*Evaluation Assurance Levels (EALs)* are formed from a taxonomy of assurance classes, families, and components defined in CC standard Part 3. There are seven hierarchically ordered EALs increasing in assurance that serve to provide general-purpose assurance packages.

*Schemes* regulate and monitor CC and CCRA processes. Schemes in certificate authorizing nations issue mCC certificates for certified ICT product and additionally, oversee laboratories and their evaluation work.

*Common Criteria Recognition Arrangement (CCRA)* is an agreement signed by each CC member nation. By signing the CCRA, a nation recognizes evaluations against the Common Criteria standard performed by other CCRA member nations. Membership falls into two categories: authorizing nations and consuming nations. Authorizing nations have laboratories or facilities to evaluate and certify ICT products. A consuming nation agrees to recognize ICT products certified by other authorizing nations. An authorizing nation is also a consuming nation.

The CCRA infrastructure includes a Management Committee (CCMC) that is responsible for the management of the CCRA and a Development Board (CCDB) responsible for the management of the CC standard.

### Common Criteria – Brief History

Prior to CC nations relied upon pre-existing criteria standards for evaluating the security of ICT products:

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.

In the late 1990’s the Common Criteria standard was produced by unifying the pre-existing standards. The first major CC release came in May 1998 with the release of CC 2.0 followed by version 2.1 in August 1999. CC parts 1-3 became an International Organization for Standardization (ISO) standard in 1999 (ISO/IEC 15408) followed by the CEM which became an ISO standard (ISO/IEC 18045) in 2005.

The development of a unified Common Criteria standard paved the way for the Common Criteria Recognition Arrangement (CCRA). The aim of the CCRA was to eliminate the need for costly security evaluations in more than one nation by establishment of mutual recognition of evaluated ICT products at EALs 1-4 by all nations that officially sign onto the CCRA.

In 2007 the next significant version of the CC standard, version 3.1 was released. The current version is CC v3.1 release 4.

Statistics provided from the CC international portal as of August 2014 list a grand total of 2,434 products have been certified using the Common Criteria standard.

## Common Criteria – Areas Improving

While there are many important benefits to Common Criteria, areas exist where improvement is needed.

1. Many nations (twenty-six) now officially recognize Common Criteria. A nation recognizing evaluations against the Common Criteria standard performed by other CCRA member nations has limitations. ‘Recognition’ means the it is agreed that the certifying scheme correctly performed all of the activities involved in CC and CCRA processes. However it does not mean the certified ICT product met the security requirements of another CCRA member nation.
2. The requirements in the CC standard were written to be sufficiently flexible to allow specification of a wide range of ICT products. This has been shown to have had the unintended effect of yielding varying and/or subjective results, especially at EALs above 2. For example, evaluation results at EAL4 from a laboratory testing a firewall in one certifying scheme are very difficult to compare with evaluation results produced from an evaluation laboratory in another certifying scheme.
3. The CC was devised to ensure the evaluation fulfills the need of multiple target audiences but of particular importance is the end-user (or consumer). Customized STs with an EAL designation typically claim security requirements asymmetrically from one another as a common minimum bar technologies need to meet is not defined. This leaves the end-user wrestling with the arduous task of finding certified ICT product that will meet their security needs. End-users
4. need a voice in the process to collaborate on the certified security features in a technology that will meet their minimum risk tolerance.

Another end-user complaint is the evaluation process takes too long while product vendors often say the evaluation costs are too high. Industry changes that bring new vendor technologies, development approaches, and shorter time to market serve to exacerbate these problems.

To address these needed improvements the CCRA Management Committee (CCMC) announced in September 2012 a shift is needed away from harmonizing the CC/CEM processes among divergent national schemes and instead focus on development of new-style Protection Profiles called *Collaborative Protection Profiles* or cPPs. cPPs are developed by *International Technical Communities* or iTCs. cPPs move away from Protection Profiles of the past that were developed without strong engagement of all CCRA participant nations.

## iTCs and cPPs – Defining Common Minimum Requirements for Technologies

An iTC is a structure to discuss and agree upfront on what are common minimum security requirements and reasonable assurances for a technology to mitigate the top-level threats it faces. Rather than establishing criteria standards in closed-door government settings, iTCs bring in an open international forum the skills, expertise, and security knowledge from all stakeholders in the evaluation. iTCs are composed of but not limited to:

* Scheme experts
* Product vendors
* Consultants and Evaluators
* Government end-users

International Technical Communities (iTCs) create a Collaborative Protection Profile (cPP) and associated supporting documentation for technologies of national interest to participant CCRA nations. Using the framework of the CC standard, a cPP will define the minimum set of common security functional requirements for technology types.

In addition rather than using general-purpose assurance packages predefined in an EAL structure, iTCs will utilize the taxonomy of assurance classes, families, and components defined in CC standard to create an achievable level of assurance tailored where necessary to the technology type. This will result in a level of assurance that will repeatable among evaluation laboratories and facilities in any certifying scheme.

Lastly by evaluating an ICT product against a published cPP, laboratories and facilities can focus their activities that are of most concern to end-users resulting in reduced cost and length of time required for evaluation.

## CCRA Revision

The changes in the revised CCRA will permit mutual recognition of ICT products that are evaluated against a cPP.

After a transition period cPPs should be applied instead of individual STs with an EAL designation. The revised CCRA will only permit an evaluation with an EAL designation for cases where cPPs does not exist or is not applicable. CC certifications where a cPP does not exist or is not applicable will be mutually recognized only at or below EAL2.

## Summary - An Evolved CC Benefiting All Stakeholders

iTCs and cPPs that focus evaluation testing on the threats that are of most concern to stakeholders produces evaluation results that are reasonable, comparable, relevant, and cost-effective.

Incorporating the security requirements of CCRA nations into the cPP produces more meaningful evaluation results. The mutual recognition of a CC certificate is strengthened and linked to procurement processes for those nations that have national requirements for the technology. This increases the global market value of the Common Criteria for all stakeholders and ensures certified ICT products reach a worldwide common-level of security.

The benefits of an evolved CC standard outlined in this paper are summarized below:

1. *Relevant – iTC to develop, maintain, and update collaborative protection profiles that meet the security concerns of end-user.*
2. *Recognized - Security requirements appropriate to end-user needs and differing technologies that are recognized across 26 nations.*
3. *Repeatable – Evaluation results that are comparable and reproducible.*
4. *Reviewed – Authorized laboratories or facilities provide independent review to ensure the product performs as designed/advertised.*
5. *Reasonable – Timely evaluations ensure end-users get evaluated products shortly after general release.*
6. *Revealing – Requirements are developed transparently in open and collaborative technical communities.*

For additional information refer to:

The Common Criteria Users Forum: <http://www.ccusersforum.org/>

The International Common Criteria Portal: <http://www.commoncriteriaportal.org/>