



## IT Product Certification Programs: Are they useful?

Mr. Keith Beatty and

Mr. J. Mark Braga

Science Applications International Corporation

Common Criteria Testing Laboratory

March 22, 2006

---

### Abstract

Since July 2002, all commercial off-the-shelf (COTS) information assurance-enabled Information Technology (IT) products to be used on the systems specified in the National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) must be evaluated and validated in accordance with the criteria, schemes, or programs specified. This paper will briefly review of the past two decades of certification efforts, examine the impact of NSTISSP-11 on the current certification climate for products and technology, and speculate on the continuing evolution of certification efforts with respect to shifts in the current paradigm.

### Introduction

Certification is becoming a commodity in the Information Assurance (IA) Information Technology (IT) arena – a check list item indicating inclusion in a pre-determined group of software and hardware products all of which have been evaluated to a particular standard; it is quite similar to receiving a Underwriters Laboratories (UL) approval (a trusted source “across the globe for product compliance.”). Although certification of Network security products would not, necessarily, include the kind of product safety tests that has made the UL famous for more than a century, certification (of network security products) does imply a level of assurance that they will behave in a predictable manner and/or that they will adhere to a pre-determined set of requirements. Because the accurate demonstration and enforcement of best practices and/or compliance standards is prohibitively expensive and difficult when performed individually, an internationally recognized certification program such as the Common Criteria (CC) or the Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules can serve as a benchmark/check-mark for organizations seeking an accredited “placeholder” from which to start the crucial and often tedious product evaluation process that frequently culminates in complex purchase decisions. Certification is, therefore, not directed at research but rather at the application and implementation of technology as expressed in commercial off the shelf (COTS) products used

in government (principally) as well as commercial venues.

Certification in the context of network security means that the system has been analyzed as to how well it meets all of the security requirements that have been levied against it from various sources. The relationship between certification/accreditation and the information network system is a life cycle commitment that is frequently misunderstood. [15]

Having software rated against well-defined standards helps governments, corporations, and end-users protect information. This information may be expressed through physical asset security or through electronic means in its many flavors and expressions. Preventing unauthorized access to sensitive data is “essential in any environment in which multiple users have access to the same physical or network resources.” [21]

Since July 2002, all COTS information assurance-enabled IT products to be used on the systems specified in the National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) must be evaluated and validated in accordance with the criteria, schemes, or programs specified. The IA Technical Considerations Section (7.5.9.5) of Department of Defense (DoD) Directive 8500.1 requires COTS IA and IA-enabled products as part of any DoD IT security architecture. These products must be NSTISSP-11 compliant, requiring them to be validated by accredited labs under the National Information Assurance



Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP). [5]

### A Brief History of Time

The National Computer Security Center (NCSC)<sup>1</sup> was established in 1981 as part of the DoD National Security Agency (NSA). One of the NCSC goals was to create a range of security ratings that could be used to indicate protection levels offered by commercial operating systems, network components, and trusted applications. In December, 1985 these ratings were set forth in a DoD Standard (DOD 5200.28-STD) entitled the Department of Defense Trusted Computer System Evaluation Criteria which came to be referred to as the “Orange Book”, or the TCSEC standard.<sup>2</sup>

TCSEC gave rise to a European counterpart, the Information Technology Security Evaluation Criteria (ITSEC). In May 1990, [France](#), [Germany](#), the [Netherlands](#) and the [United Kingdom](#) published the Information Technology Security Evaluation Criteria (ITSEC) based on existing work in their respective countries. Following extensive international review, Version 1.2 was subsequently published in June 1991 by the [Commission of the European Communities](#) for operational use within evaluation and certification schemes. ITSEC was a structured set of criteria for evaluating computer security within products and systems. Each evaluation involved a detailed examination of IT security features culminating in comprehensive and informed functional and penetration testing.

Predictably, the efforts of these two certification bodies, along with a Canadian initiative (CTCPEC) left vendors, as well as consumers, of international breath with competing standards (certifications). With the rise throughout the 1990s of networking as a dominant component in the global IT market, in conjunction with proliferation of Winware, Open systems models of client server computing, and the expansion of

the Internet, pressure was brought to bear on these certification bodies to find an acceptable methodology for mutually recognizing evaluated (certified) products; this gave rise to the CC.

The CC<sup>3</sup>, “is an international initiative by the following organizations: CSE (Canada), SCSSI (France), BSI (Germany), NLNCSA (Netherlands), CESG (UK), NIST (USA) and NSA (USA). It represents the outcome of efforts to develop criteria for evaluation of IT security that are widely useful within the international community. It is an alignment and development of a number of source criteria: the existing European, US and Canadian criteria (ITSEC, TCSEC and CTCPEC respectively).” [4] Version 1.0 of the CC was published for comment in January 1996. The CC v2.2 has also been published as an ISO/IEC 15408:2005 and ISO/IEC 18405:2005 standard. The current version of the CC is 2.3.

### NSTISSP #11

The impact of NSTISSP-11 and DoD 8500 on the current COTS IT security product certification climate is instructive. To date, approximately 140 IT security products have been CC certified and another 150 are “in evaluation.” All these certifications and current evaluations have a common market delineator: the DoD.

At roughly \$30.5 billion, defense spending accounts for almost one-half of all federal IT spending in the 2007 budget; homeland security spending will account for another \$12.4 billion. [14] According to one source within SAIC, the size of direct Department of Defense IT spending is estimated to be 8 percent, or \$5.1 billion of the federal IT market. Of this figure approximately 90% of that market is comprised of COTS products. It is this market that is directly impacted by NSTISSP-11, the DoD directive 8500.1, and the DoD instruction 8500.2 which sets the requirement for CC certification.

In an [IAnewsletter](#) article from 2001 entitled “Life Cycle Security and DITSCAP”, the authors stated that “With the announcement of the Department of Defense (DoD) will be spending \$1.5 billion on information security, many organizations, both public and private, have presented themselves as experts in network security in order to take advantage of this

<sup>1</sup> Available at [www.radium.ncsc.mil/tpep/](http://www.radium.ncsc.mil/tpep/)

<sup>2</sup> Available at <http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html>

<sup>3</sup> Available at [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org)

windfall. But posturing does not guarantee professional results and, in reality, many of those claiming to be security engineers and certifiers/accreditors have little in-depth experience in the field. In some cases, organizations are not familiar with DoD or federal department-specific regulations. They cannot relate to the manner in which the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) should be applied. Only an informed community can separate the nascent from the experts.” [15]

What is to be made of the effort to certify individual security specialists? According to one Microsoft spokesperson, “We believe that independent certification of security professionals is an important thing.” [19] Certification of network security products would then seem to beg the question, “If people need to be certified why aren’t the products that they use, recommend, install, and support held to the same level of scrutiny?”

The key points of NSTISSP #11<sup>4</sup> are summarized below [18]:

- NSTISSP #11 is a critical policy component of the U.S. Government's overall Information Assurance (IA) strategy. It is imperative that policies and processes be established to validate the performance claims of marketed IA products, and to ensure that these products are responsive to the security needs of the intended user. In the context of national security systems and information, these requirements take on added significance and importance. NSTISSP #11 is a binding, national policy requirement.
- NSTISSP #11 is a national security community policy governing the acquisition of information assurance (IA) and IA enabled information technology products. This policy was issued by the Chair of the National Security Telecommunications and Information Systems Security Committee (NSTISSC), now known as the Committee on National Security

---

<sup>4</sup> A more extensive explanation of NSTISSP #11 can be found at <http://niap.nist.gov/cc-scheme/nstissp-faqs.html>

- Systems (CNSS) in January of 2000 and revised in June, 2003.
- The policy mandated, effective 1 July 2002, that departments and agencies within the Executive Branch shall acquire, for use on national security systems, only those COTS products or cryptographic modules that have been validated with the International Common Criteria for Information Technology Security Evaluation, the NIAP CCEVS, or by the NIST Federal Information Processing Standards (FIPS) [Cryptographic Module Validation Program](#).
- The objective of NSTISSP #11 was to ensure that COTS IA and IA-enabled IT products acquired by the U.S. Government for use in national security systems perform as advertised by their respective manufacturers, or satisfy the security requirements of the intended user. To achieve this objective, the policy requires COTS products be evaluated and validated in accordance with either the International Common Criteria for Information Technology Security Evaluation, or the NIST Federal Information Processing Standard (FIPS) 140-2. Supportive of the intent and implementation of NSTISSP #11, the NSA and NIST have collaborated to establish the following two evaluation and validation programs: The [National Information Assurance Partnership's \(NIAP\) Common Criteria Evaluation and Validation Scheme \(CCEVS\)](#) Program and the [NIST Federal Information Processing Standard \(FIPS\) Cryptographic Module Validation Program \(CMVP\)](#) each which target different, but complementary, areas.
- NSTISSP #11 applies to all departments and agencies in the Executive Branch that acquire COTS products for use in national security systems.
- NSTISSP #11 applies to products being acquired for national security systems used to enter, process, store, display, or transmit national security information.
- A COTS IT product is widely available and is developed with general commercial applications in mind. Such

products typically have little or no U.S. Government funding or influence.

- An IA product is an IT product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control and non-repudiation of data); correct known vulnerabilities; provide layered defense against various categories of non-authorized and malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls and intrusion detection devices.
- The advantages of using international standards are that commercial vendors (either domestic or foreign) are not limited to having their products tested within their own countries. Any commercial testing laboratory accredited as compliant with the [Common Criteria Recognition Arrangement](#) (CCRA) can perform evaluations up to and including evaluations at the EAL 4 level. This arrangement ensures that accredited laboratories, regardless of their geographic location or national affiliation, will test products against the same criteria and use the same testing methodology.

### **DoD 8500 - the Waterfall Model, or “You Can’t Get There From Here”**

When DoD Directive 8500.1<sup>5</sup> became effective on October 24, 2002, it called for information assurance requirements to be identified and included in the design, acquisition, installation, operation, upgrade, and replacement of all DoD information systems. [6] The central thrust of this directive can be found in paragraph 4.17 which effectively mandates a CC certification for all IA related purchases as they pertain to DoD information systems. “All IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DoD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 ((NSTISSP) No.11,

---

<sup>5</sup> Available at <http://niap.nist.gov/cc-scheme/policy/dod/d85001p.pdf>

“Nation Policy Governing the Acquisition of IA and IA-enabled Information Technology Products,” January 2000) [7].

Subsequently, DoD Instruction 8500.2<sup>6</sup> became effective on February 6, 2003. This instruction provides the detail necessary to implement and enforce DoDD 8500.1 policy. Briefly stated, instruction 8500.2 employs a waterfall model to direct the acquisition of IA products. This starts with the establishment of protection profiles. “The Director of the National Security Agency shall Generate PPs for IA and IA-enabled IT products used in DoD information systems based on Common Criteria (reference (j)), and coordinate the generation and review of these Profiles within the NIAP framework.” [8]

However, the acquisition cascade that restricts purchase to CC certified products lies in Section E3.2.5 (Product Specification and Evaluation) and its subparagraphs as stated below.

E3.2.5. Product Specification and Evaluation. At the enterprise level, implementation-independent specifications for IA and IA-enabled IT products are provided in the form of protection profiles. Protection profiles are developed in accordance with the CC (reference (j)) within the NIAP framework. Regardless of the mission assurance category or confidentiality level of the DoD information system, all incorporated IA products, and IA-enabled IT products that require use of the product's IA capabilities, acquired under contracts executed after July 1, 2002, shall comply with the evaluation and validation requirements of NSTISSP No. 11 (reference (National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, “National Policy Governing the Acquisition of IA and IA-Enabled Information Technology Products,” January 2000)<sup>7</sup>, with the following qualifications:

E3.2.5.1. If an approved U.S. Government protection profile exists for a particular technology area and there are validated products available for use that match the protection profile description, then acquisition is restricted to those

---

<sup>6</sup> Available at <http://niap.nist.gov/cc-scheme/policy/dod/d85002p.pdf>

<sup>7</sup> Available at <http://www.nstissc.gov/html/library.htm>

products; or to products that vendors, prior to purchase, submit for evaluation and validation to a security target written against the approved protection profile. Products used within the Department of Defense may be submitted for evaluation at evaluation assurance levels (EALs) 1-7 through the NIAP CCEVS. Alternatively, the United States recognizes products that have been evaluated under the sponsorship of other signatories and in accordance with the International Common Criteria for Information Security Technology Evaluation Recognition Arrangement (CCRA) for EALs 1-4 only.

E3.2.5.2. If an approved U.S. Government protection profile exists for a particular technology area, but no validated products that conform to the protection profile are available for use, the acquiring organization must require, prior to purchase, that vendors submit their products for evaluation and validation by a NIAP EVP or CCRA laboratory to a security target written against the approved protection profile or acquire other U.S.-recognized products that have been evaluated under the sponsorship of other signatories to the CCRA.

E3.2.5.3. If no U.S. Government protection profile exists for a particular technology area and the acquiring organization chooses not to acquire products that have been evaluated by the NIAP CCEVS or CCRA laboratories, then the acquiring organization must require, prior to purchase, that vendors provide a security target that describes the security attributes of their products, and that vendors submit their products for evaluation and validation at a Defense Approving Authority (DAA) approved EAL. Robustness requirements, mission, and customer needs will together enable an experienced information systems security engineer to recommend a specific EAL for a particular product to the DAA.

E3.2.5.4. Acquiring DoD organizations that anticipate using the IA functionality of subsequent versions of an evaluated product shall specify in the original contract that product validation will be kept current through vendors submitting the next version of their products for evaluation or through participation in the NIAP Assurance Maintenance Program or the CCRA Assurance Maintenance Program.

E3.2.5.5. Products that are available under multiple-award schedule contracts or non-DoD

Government-Wide Acquisition Contracts (For example, GSA schedules and other contract vehicles established by other Federal Departments or Agencies that are available for DoD use.) awarded before July 1, 2002, must be evaluated when and if a version release of the product is made available under the contract.

E3.2.5.6. Although products that have not satisfactorily completed evaluation may be used, contracts shall require that any evaluations initiated under the conditions described in subparagraphs E3.2.5.1. through E3.2.5.5., above, must be satisfactorily completed within a specified period of time.

E3.2.5.7. Implementation of security-related software patches directed through the DoD IAVA program shall not be delayed pending evaluation of changes that may result from the patches.

The following list summarizes the implications of Section E3.2.5 and its subparagraphs [6]:

- Section E3.2.5: implies that all Business Systems Modernization (BSM) IA and IA-Enabled COTS products purchased after July 1, 2002 must be validated and certified in accordance with the CC regardless of their mission assurance category or robustness level.
- Section E3.2.5.1: A protection profile (PP) is a generic set of security requirements for a specific technology e.g. firewalls. Acquisition of a product is restricted to those products that have already been certified under a US government approved PP or those that are submitted for evaluation and validation by the vendor prior to purchase. The US only recognizes products certified for EALs 1-4 outside the US. Products requiring EAL 5 and higher must be certified by the NIAP CCEVS (US CC evaluation scheme).
- Section E3.2.5.2: If a PP exists for a specified technology but no validated product/s exist under this PP within the NIAP CCEVS, the vendor needs to
  1. submit their product/s for CC evaluation and verification prior to the purchase being executed and
  2. submit a security target (implementation dependent specification of the security

- required, both functionality and assurance) for the product/s against the approved US government PP
- Section E3.2.5.3: If a no PP exists for a specified technology and the acquiring organization chooses not to purchase a product evaluated by NIAP CCEVS or CCRA, then the acquiring organization must require proof from the vendor that,
    1. the vendor submitted their product/s for CC evaluation and verification at a DAA approved EAL prior to the purchase being executed and
    2. the vendor submitted a security target describing the security attributes of their product/s.
    3. The acquiring organization based on their needs, robustness level and mission will recommend an EAL for the required IA or IA-Enabled product for their organization.
  - Section E3.2.5.4: If the acquiring organization anticipates using subsequent versions of an evaluated product, they need to specify wording in the original contract that requires the vendor of the product to keep subsequent versions of their product/s validated through the NIAP CCEVS Maintenance Program<sup>8</sup> or the CCRA Maintenance Programs<sup>9</sup>.
  - Section E3.2.5.5: The CC evaluation requirement applies to new versions of products available after July 1, 2002 under the above DoD and non-DoD government-wide contracts.
  - Section E3.2.5.6: The paragraph implies that the acquiring organization must specify a time period in the original contract signed with a vendor within which the product in question will satisfactorily undergo a CC evaluation.

---

<sup>8</sup> Available at [http://niap.nist.gov/cc-scheme/Pub6\\_v1.pdf](http://niap.nist.gov/cc-scheme/Pub6_v1.pdf)

<sup>9</sup> Available at [http://www.commoncriteria.org/review\\_docs/docs/AMAv09.pdf](http://www.commoncriteria.org/review_docs/docs/AMAv09.pdf)

- Section E3.2.5.7: This implies that the implementation of software patches that are directed by the DoD IA Vulnerability Assessment (IAVA) program for a CC evaluated product will not be delayed due to CC evaluation pertaining to the changes.

The waterfall model described in Section E3.2.5 of 8500.2 is further illustrated by Figure 1, the IA Compliance Decision Tree below. Taken from Chapter 7 of the Defense Acquisition Guidebook, this flowchart indicates that there is only one branch that does not invoke the 8500.1 (certification) policy as described in Section E3.2.5 of the 8500.2 instruction above.

### **Caveat Emptor**

The main certifications for security products are the CC, the Federal Information processing Standard 140-2 (FIPS 140-2) Security Requirements for Cryptographic Modules, and International Customer Service Association (ICSA) Labs.

The CC is an assurance evaluation process, culminating in a certificate, whereby IT security products are evaluated against the security functional and assurance requirements of a Protection Profile (PP) and/or a Security Target (ST). PPs may be developed by users of the product (typically government) and apply to a specific product class and the expected security requirements of that class. For example, the Controlled Access PP applies to operating systems and replaces the old C2 evaluation requirements from the Orange Book. The CC also specifies a series of Evaluation Assurance Levels (EALs) for evaluated products. A higher EAL certification specifies a higher level of assurance (confidence) that a product's security functions will be performed correctly, effectively, and corrected and maintained.

CC security functional requirements apply to IA & IA-enabled IT products that are incorporated into DoD information systems. They form an engineering language and method for specifying the security features of individual IT products, and for evaluating the security features of those products in a common way that can be accepted by all. [8]

Furthermore, in the Security Design and Configuration subject area of DoD Instruction 8500.2, the DCAS-1 Acquisition Standards states that, “The acquisition of all IA- and IA-enabled GOTS IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes. The

acquisition of all IA- and IA-enabled COTS IT products is limited to products that have been evaluated or validated through one of the following sources - the International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and

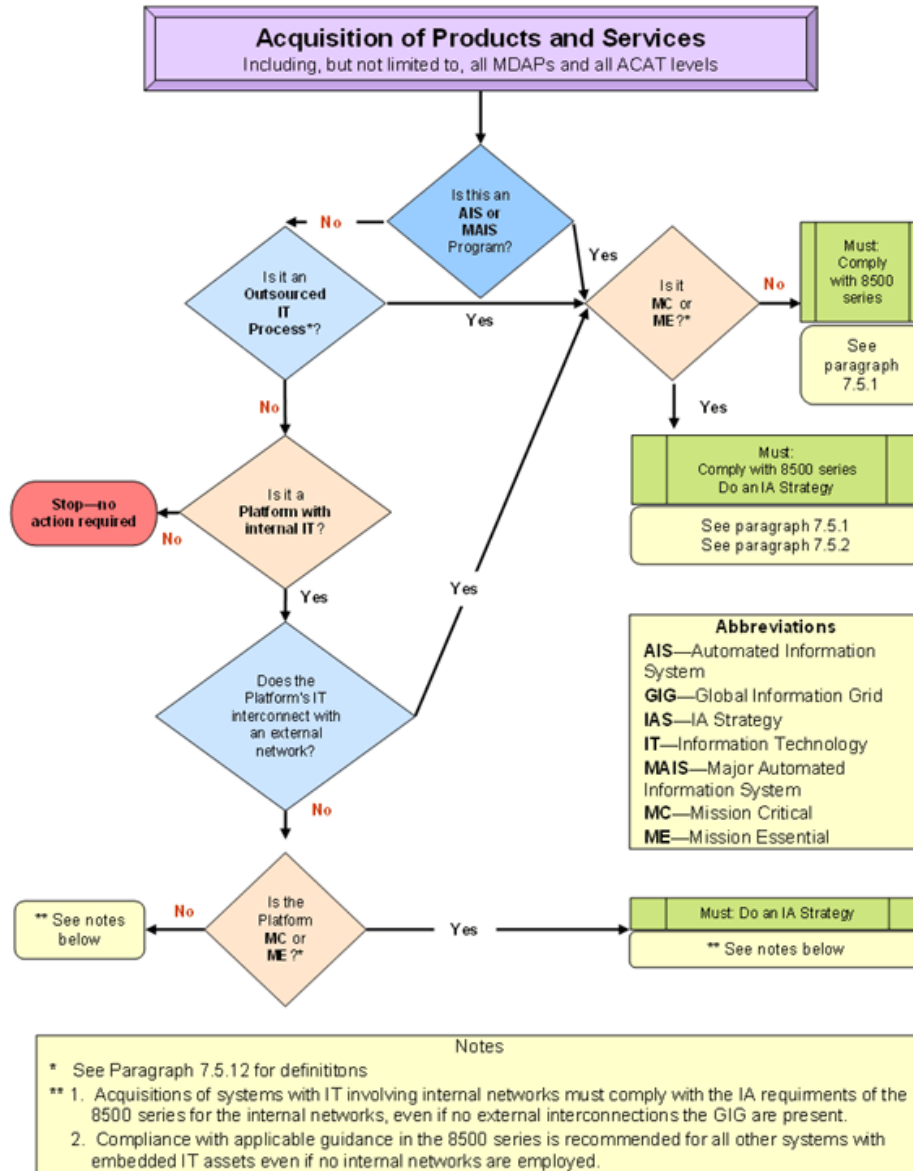


Figure 1: IA Compliance Decision Tree [5]

Validation Program, or the FIPS validation program. Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a PP, a particular evaluated product, or a security target with the appropriate

assurance requirements for a product to be submitted for evaluation.” [8]

FIPS 140-2 is a certification for cryptographic modules sponsored by the NIST. NIST-approved labs test new products to the FIPS 140-2 standard which ensures that cryptographic subsystems are implemented correctly and provide for an adequate level of protection for stored, sensitive data. [11] It is an [information technology security accreditation program](#) for cryptographic modules produced by private sector vendors who seek to have their products certified for use in government departments and regulated industries (such as financial and health-care institutions) that collect, store, transfer, share and disseminate sensitive, but not classified information.

ICSA Labs tests and certifies cryptographic software, firewalls, antivirus software and IPsec VPN software and appliances against published documents and other products. An ICSA Labs certification is functional testing with pass/fail components. The certification criteria are compiled from security vendors and experts in the field. Unlike the CC, ICSA Labs' industry certification does not include implementation guidelines and environmental constraints; the tests don't take into account architectural differences of a product or its internal protection enhancements. [11]

ICSA Labs<sup>10</sup> is an independent commercial division of Cyber trust, Incorporated. It has been a research, intelligence, and certification testing authority for security products. ICSA Labs has standards for information security products and certifies over 95% of the installed base of anti-virus, firewall, IPsec VPN, cryptography, SSL VPN, network IPS, anti-spyware and PC firewall products commonly deployed in the world today.

While these certifications tend to complement each other, for the government, specifically the DoD space, the CC and FIPS 140-2 are the two programs that matter, as per NSTISSP-11 policy.

With any certification, it is important to remember that a certified product does not necessarily imply one that is more secure than an uncertified one. "It may be that the vendor of the uncertified product has not yet submitted it for testing or that testing is still under way." [11] Certifications are good at capturing a common set of requirements. However, test results

represent a specific point in time and may be rendered obsolete rather abruptly. What certification delivers is assurance that the product has been tested and has passed a specific set of tests and evaluation criteria. Such assurance may be helpful to government and industry as they select security products to protect sensitive networks and data.

### **Protection Profile, Security Target, and the Target of Evaluation (PP, ST, and TOE)**

The CC presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. The CC defines a PP construct which allows prospective consumers or developers to create standardized sets of security requirements. A PP defines an implementation-independent set of security requirements and objects for a category of products or systems which meet similar consumer needs for IT security. A PP is intended to be reusable and to define requirements which are known to be useful and effective in meeting the identified objectives. [24] PPs are useful when a government wishes to specify security requirements for a class of security products, a consumer group wishes to specify security requirements for an application type, or an organization wishes to purchase an IT system to address its security requirements.

A ST contains a security criteria specification for a product, which can be derived from the security criteria in a PP or it can be self-defined. When a ST claims compliance to a PP, part of the CC evaluation process verifies conformance between the criteria in the ST and the PP.

The Common Evaluation Methodology (CEM) specifies a set of steps for validating the assurance requirements in a ST. The CEM addresses only assurance levels EAL1 through EAL4 - and these are the only assurance levels that are mutually recognized. Higher assurance levels (EAL5-7) may be obtained, but in the U.S., requires the participation of the National Security Agency (NSA) to work with the CCTL. Such evaluations are not mutually recognized.

The Target of Evaluation (TOE) is that part of the product or system which is subject to evaluation. The TOE security threats, objectives, requirements, and summary specification of security functions and assurance measures

---

<sup>10</sup> Available at:  
<https://www.icsalabs.com/icsa/icsahome.php>

together form the primary inputs to the ST, which forms the basis of the evaluation. The principle inputs to an evaluation are the ST, the set of evidence about the TOE, and the TOE itself. The ST may claim conformance to one or more PPs and forms the basis for an evaluation. An ST is required when submitting a product for evaluation, or when submitting a product to a consumer as a statement of the TOE's security functional and evaluated configuration.

There are eleven functionality classes in the CC: audit, cryptographic support, communications, user data protection, identification and authentication, security management, privacy, protection of the TOE Security Functions, Resource Utilisation, TOE Access, and Trusted Path. Each class consists of families; each family consists of components. Part 2 of the CC documentation contains the catalogue of functional components. Security functional components are used to express a wide range of security functional requirements within PPs and STs.

The CC contains a set of defined assurance levels constructed using components from the assurance families. The EALs define a scale (EAL1 to EAL7) for measuring the criteria for the evaluation of PPs and STs. The seven hierarchically ordered EALs increase in assurance across the levels by substituting hierarchically higher assurance components from the same assurance family, and by the addition of assurance components from other assurance families. [24] As of 29Jan06, there are 36 Validated PPs listed by CCEVS<sup>11</sup>; there are over 125 products listed on the CCEVS Validated Products List (by Technology Type)<sup>12</sup>.

### **From “Standard” to “Certification”**

Consider the following statement: “The main purpose of defining an architecture is to try to impose order on chaos, or potential chaos. Architecture is an essential first step to orderly solutions to problems. It does this by establishing a framework within which to solve both current and anticipated problems.” [1] If one were to substitute “certification” for

<sup>11</sup> Available at <http://niap.nist.gov/cc-scheme/pp/index.html>

<sup>12</sup> Available at [http://niap.nist.gov/cc-scheme/vpl/vpl\\_type.html](http://niap.nist.gov/cc-scheme/vpl/vpl_type.html)

“architecture”, the statement could be modified to read: The main purpose of certification is to try to impose an order on products. Certification is an essential first step in providing orderly comparisons by establishing a framework within which to both categorize and compare IT products. To put this in more vendor-centric terms, “It’s simple...If you run the certification environment, your product will be clearly understood to meet all the requirements. And in a crowded marketplace, that’s a pretty big thing.” [10]

In the computer industry, standards play an important role by enforcing security baselines and enabling compatibilities among products. In the best of worlds, standards provide a neutral ground where methodologies are established that advance the interests of manufacturers, as well as consumers, while providing assurances of safety and reliability. [17]

“Without standards, a technology cannot become ubiquitous, particularly when it is part of a larger network.” [23] While the author was referring to software standards such as TCP/IP, HTML, SOAP, et.al., the message remains virtually the same for certification efforts. Without certifications, there is less of a benchmark against which to differentiate products in an open market. Technology becomes less easy to transfer between market segments thereby limiting the potential size of a market by confining the product to a reduced subset of possible opportunities.

The CC defines general concepts and principles of IT security evaluation and presents a general model of evaluation. The CC is compliant with the ISO/IEC 15408 international standard. It is one of the principal, if not the principal, standards against which both software and hardware products (which include network security software and hardware - as well as network appliances) are certified.

The goal of the CC is a successful evaluation assurance process culminating the receipt of a certificate for a vendor’s successfully evaluated product; the NIAP CCEVS is the standards body that “certifies” the results of evaluations against the CC “standard” for IA. For purposes of this discussion, the terms “standard” and “certification” are interchangeable.

### **Ruminations on the Future**

While the focus of this paper has been the impact of certification on the purchase of IT products for government, specifically DoD, use, it is important to acknowledge the potential influence of the commercial sector, as well as the impact of certification in this space. According to an April, 2003 article in Total Telecom Magazine, “secure network services could prove to be a lucrative market for service providers” but providers are missing out because “they lack the certification and security management practices”. The article further states that one of the recognized standards which could help to sell additional security services, including monitoring and network management, to a marketplace expected to reach approximately \$9 billion in FY06 is the Common Criteria. [3] Additionally, a report by independent market analyst Datamonitor, Inc in 2004 predicted that global enterprise investment in firewall and virtual private network (VPN) solutions would reach almost \$6 billion in 2007. [12]

Information security (also referred to as cyber security) is characterized as the protection of information against unauthorized disclosure, transfer, modifications, or disclosure, whether accidental or intentional. [9] Networking is the key to the flow of information; network security gives structure to this key. Shortly after the millennium, International Data Corporation (IDC) predicted that the size of the worldwide market for IT security products would reach \$21 billion by 2005. [9] The demand for these products can only increase. In the fall of 2004, a study of the effect of internet security breach announcements on the market value of the announcing firm indicated an average loss of 2.1 percent of market value within two days of the announcement. [2]

Individually, each of these statements has a certain financial significance and implication. Yet, when taken as a whole, they are more indicative of a commercial sector that has gone largely unnoticed by virtue of the DoD’s emphasis on CC requirements. It is the DoD and the NSA which control PP creation and the evaluation process.

The potential for a broader certification effort in the commercial space appears, at the present time, to be largely to be undefined. However, it is possible that this may be starting to change.

When the E-Government Act (Public Law 107-347) was passed by the 107<sup>th</sup> Congress and signed into law by the President in December 2002, Title III of this Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to “develop, document, and implement an agency-wide information security program to provide information security for the information and information systems.” [20] In order to mitigate certain costs with the program area pertaining to certification and accreditation, commercial product testing, through programs such as the CC, may be employed. Additionally, in the security certification phase, CC validations may be used as supporting documentation necessary for the assessment of security controls in the information system. [20]

The CC is now 10 years old. Compared to the lifecycle of the TCSEC, its predecessor, it may now be considered as “middle-aged”. This is not necessarily a detriment. It implies a certain level of stability and predictability within the certification process; in many ways, the CC is now a mature and procedurally well understood. As such, the CC should continue to exist and proceed with a slow evolution for the foreseeable future. Version 3 is now undergoing (peer) review; version 3.1 is in its planning stages. How long the current paradigm lasts is open to speculation beyond the reach of this discussion. However, that longevity, and its influence as a certification methodology, is directly influenced, from a US participatory perspective, by the actions of the Federal government, in both its DoD as well as its non-DoD, that is, commercial components.

The TCSEC was over 15 years old before it was effectively superseded by the CC as a broader, international certification paradigm. That more than 20 countries would invest time and effort in an international certification effort would also imply continued longevity for the CC in some recognizable form, perhaps beyond the effective lifespan of the TCSEC and ITSEC. This can be construed as a strength as well as a weakness. The strength lies in the international community’s investment in defining a set of standards that provide not only a common methodology but allow for mutually recognized results. The weakness lies, as with most standards/certification efforts, in the pace at which the CC is able to adapt those standards to meet the constant challenges of a dynamic

industry; the networking space, and particularly the networking security space, will continue to evolve products and trends that will, in turn, define other new products and trends. One of the greatest challenges for the CC, or whatever passes for the CC in the future, will be to identify, catalogue, and differentiate that which is new from that which already exists.

As networking and the security for networks continue to evolve, an increase in the already rapid development of products, particularly those serving the commercial sector, nationally as well as internationally, will continue. This may lead to increasing pressure from commercially driven customers, as well as vendors, for standards/certifications that align with business goals and initiatives – global as well as national. Such pressure may have the effect of splintering the current technology types for network appliances and (network) software as currently expressed through the CC’s PPs and the CCEVS validated product types<sup>13</sup> whereby products for the commercial space are evaluated by PPs written to commercial standards while DoD requirements would retain the current PP model. This type of product divergence would ultimately require a divergence in the current accreditation body where the NSA would continue to control the DoD certification process and another governmental body, perhaps NIST, would be charged with maintaining any commercial evaluation processes. PPs produced by NIST for the commercial space would be representative of an open/OSI model whereas the NSA PPs would, effectively, be closed.

The world, particularly since 9/11, is becoming one in which all things security receive primary emphasis. The internationalization of IT is rapidly producing a global marketplace in which commercial interests, backed by increasingly rigorous security standards, may begin to set the certification pace, outstripping the dictates of the standard CC (or other) process by either combining in small groups to write protection profile-like documents that serve as de facto “industry” standards, or writing stand-alone requirements documents each with the intent of indicating to potential markets that which distinguishes, as well as certifies, a product or product type.

---

<sup>13</sup> The CC evaluated products list is available at [http://niap.nist.gov/cc-scheme/vpl/vpl\\_type.html](http://niap.nist.gov/cc-scheme/vpl/vpl_type.html)

Moving beyond direct government influence can be construed as being symptomatic of a maturing industry. The commercial sector, with the backing from Congress through FISMA, and not the DoD, may be in a position to drive the next iteration of certification standards. These may not be all that different from those that have been established for the DoD; “new” may not be required if the “old” can be recycled.

Individual companies may attempt write their own PPs to gain competitive advantage. While this may appear, superficially, to be a case of altruism run amok, the commercial space is a large and relatively untapped area for certification. If a goal of the CC has been to provide give vendors with a way to internalize development and to learn how to implement security, then should vendors be able to internalize the implementation of security and security practices, using the CC as a template, it may be possible to imbed security practices into product development in a manner that would become consistent and easily recognizable by potential customers.

Altruism aside, the possibility does exist for CC certifications to be used as leverage in the commercial space. Commercial security interest tends to be audit-centric. The DoD is far more concerned with the ability of products to deny access to an object. However, the CC provides for the inclusion of an audit assurance class. In the current CC paradigm, if an evaluated product includes an audit component, then it may be possible to argue the applicability of the evaluation process that resulted in a CC certification as a commercial market differentiator regardless of whether the product is currently being utilized solely in a DoD environment. If a product is good enough for the NSA there would seem to be a reasonable expectation that it would also be good enough for use in most, if not all, commercial sectors.

In the short term, certification through the CC will continue to be advanced, in the US, by mandate of the Federal government. Any company wishing to respond to DoD RFPs must comply with the instructions on information assurance in the 8500 series of DoD publications. This means that all products – hardware and software – must attain a CC certification in order to satisfy the IA Technical Considerations portion of an Acquisition strategy. Where once the phrase “you can’t get

there from here” was the tag line to any of a number of jokes about directions through rural America, it is now all the more relevant, and required, for vendors wishing to successfully respond to DoD requirements.

## Conclusion

Thomas Kuhn, in his essays entitled The Structure of Scientific Revolutions, stated, “...it should be easy to design a list of criteria that would enable an uncommitted observer to distinguish the earlier from the more recent theory time after time. Among the most useful would be: accuracy of prediction, particularly of quantitative prediction...Less useful for this purpose...would be such values as simplicity, scope, and compatibility with other specialties...Later scientific theories are better than earlier ones for solving puzzles in the often quite different environments to which they are applied.” [16]

The same holds true in the field of Network Security. As this field inevitably matures both as a business and as an industry, it will also continue to evolve, allowing an observer to differentiate between historical (TCSEC/ITSEC) and current (CC, et.al.) efforts. As IT has come to emphasize the operating system less and the network (and the database) more, this natural evolution can be partially expressed through an

increased pace in the continuing march of certification which produces a level of compatibility, if not simplicity. The CC is better suited to solving the puzzle of international certification and cooperation than was its predecessors which operated more in a regional, if not a national, environment.

The future will present an increasing number of opportunities to address new and on-going challenges put forth by such a business and industrial model. It is important to remember, however, that the evolution of computer security standards should be considered dynamic rather than static in order to best reflect the constantly changing environments in which they are being deployed. [17]

In the end, it will be those individuals – vendors – who, working in concert with consumers and possessing the proper tools, will be able to produce products that take fuller advantage of the opportunities that the challenges of networking and network security will continue to identify and create. Certification well defined, regardless of type or forum, will, when properly utilized, become an even more powerful tool enabling sellers, as well as buyers, of all things networking to successfully respond to the requests of the present while helping to anticipate the rapidly changing and increasing complex challenges to, and for, network security.

---

## References

- [1] Britton, Chris, and Bye, Peter. IT Architectures and Middleware, 2<sup>nd</sup> Edition. Addison-Wesley. 2004.
- [2] Cavusoglu, Huseyin, Mishra, Birendra, and Raghunathan, Srinivasan. “*The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers*”. International Journal of Electronic Commerce; Fall 2004, Vol. 9, No. 1, pp. 69–104.
- [3] Collins, Jonathan. “*Certify your network*”. Telecom Magazine Apr2003.
- [4] Common Criteria: An Introduction.  
<http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf>
- [5] Defense Acquisition Guidebook. Chapter 7, “*Acquiring Information Technology and National Security Systems*”. [http://akss.dau.mil/dag/GuideBook/PDFs/Chapter\\_7.pdf](http://akss.dau.mil/dag/GuideBook/PDFs/Chapter_7.pdf)
- [6] Defense Logistics Agency. DoD Directive 8500.1 & DoD Instruction 8500.2 Overview (Draft); [http://www.eng.auburn.edu/departments/csse/classes/comp6370/resources/8500\\_1\\_8500\\_2\\_dla\\_reference.pdf](http://www.eng.auburn.edu/departments/csse/classes/comp6370/resources/8500_1_8500_2_dla_reference.pdf)
- [7] Department of Defense. Directive Number 8500.1; October 24, 2002.
- [8] Department of Defense. Instruction Number 8500.2; February 6, 2003.
- [9] Department of Information Technology. Cyber Security-Education and Awareness.  
<http://www.mit.gov.in/cybersecurity/index.asp>.
- [10] Forman, Michael. “*Funding, Older Versions Hamper Certification*”. Securities Industry News; Vol 12, Issue 5, 01/31/2000.

- [11] Fratto, Mike. “*Certification Security Blanket*”. Network Computing; 7/24/2003, Vol. 14, No. 14, p. 87-90.
- [12] “*Global Enterprise Firewall/VPN Spending to Hit \$6BN by '07*”. Computer Security Update; Apr2004, p.3-5.
- [13] Information Assurance Directorate. “Information Assurance Leadership for the Nation.” 24March2005. <http://niap.nist.gov/cc-scheme/nstissp-faqs.html>
- [14] ITAA Press Release. “ITAA Praises Bush Administration IT Budget.” 10Feb06; <http://www.ita.org/newsroom/release.cmf?ID=2251>
- [15] Kimbell, John and Walrath, Marjorie. “*Life Cycle Security and DITSCAP*”. IAnewsletter; Vol.4, No.2, Spring 01.
- [16] Kuhn, Thomas. The Structure of Scientific Revolutions. University of Chicago Press, 1970, p. 205-6.
- [17] Mecuri, Rebecca. “*Standards Insecurity*”. Communications of the ACM; Dec2003, Vol. 46 Issue 12, p.21-25.
- [18] NSTISSP #11 FAQ. <http://niap.nist.gov/cc-scheme/nstissp-11-faqs.pdf>
- [19] Richmond, Riva. The Wall Street Journal. “Thwarting Hackers Is One IT Job That Shows No Sign of Shrinking,” Nov 10, 2004.
- [20] Ross, Ron, Swanson, Marianne, Stoneburner, Gary, Katzke, Stu, and Johnson, Arnold. Guide for the Security Certification and Accreditation of Federal Information Systems. NIST Special Publication 800-37; May 2004. <http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>
- [21] Russinovich, Mark E., Solomon, David A. Microsoft® Windows® Internals; Microsoft Press, 2005, p. 485.
- [22] Schweber, Bill, Wright, Maury. “*Standard procedures*”. EDN Global Report; November, 2004. p.19-26.
- [23] Siegele, Ludwig. “*Coming of Age: A Survey of the IT Industry*”. Economist; May 10, 2003.
- [24] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model; January 2004, Version 2.2, Revision 256..