

Common Criteria: A Prime Factor in Information Security for the DoD

Kathy Malnick



**NOW MANDATORY FOR THE
DOD IS THE USE OF
INFORMATION TECHNOLOGY
PRODUCTS THAT HAVE
BEEN INDEPENDENTLY
EVALUATED AND
CERTIFIED.**

Is your vital information secure? How do you know? Are you sure? There are several ways to increase confidence in the security of your vital information. The data could be moved to a non-accessible location. A security firm could be hired to install, update, and monitor the system. But perhaps the easiest method, and one that is now mandatory for the DoD, is the use of information technology products that have been independently evaluated and certified. While this sounds like a great idea, how does one find such IT products?

The answer is that certified products are listed on the National Information Assurance Partnership (NIAP) Web site at niap.nist.gov/cc-scheme.

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) established the NIAP to evaluate information technology product conformance to international standards, namely the Common Criteria (CC). The program, officially known as the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) for IT Security, is a partnership between the public and private sectors. The program was implemented to help consumers select commercial off-the-shelf (COTS) IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace. One of the program's main objectives is to improve the availability of evaluated IT products.

Department of Defense Policies

The DoD mandated the use of evaluated IT products in October 2002, with the issuance of DoD Information Assurance Directive 8500.1, which stated that "all IA [Information Assurance] 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 #11]." This thrust DoD and its vendors into the world of CC product evaluations—the subject of NSTISSP #11. The DoD and its vendors share responsibility for compliance with Directive 8500.1, in-

Malnick, senior manager for Criterion Independent Labs at the West Virginia High Technology Consortium (WVHTC) Foundation, is responsible for Common Criteria evaluation and educational outreach efforts. She holds a bachelor's degree in computer science and a master's in software engineering.

**THE COMMON CRITERIA ARE
A SET OF FUNCTIONAL AND
ASSURANCE SECURITY
REQUIREMENTS DEVELOPED
TO PROVIDE A COMMON
INTERNATIONAL EVALUATION
BASELINE FOR IT PRODUCTS
AND SYSTEMS.**



cluding the provisions for independent product evaluations. Such evaluations require both procurement officers and vendors to understand the purpose of CC evaluations and the effort it takes to earn product certification.

Common Criteria Overview

Simply put, CC product evaluations are designed to ensure the DoD is procuring products that have been independently verified to meet their security claims. In greater detail, the CC are a set of functional and assurance security requirements developed to provide a common international evaluation baseline for IT products and systems. A full description of those requirements can be found in the International Standards Organization standard, ISO/IEC 15408.

CC product evaluations are conducted by accredited independent test labs known as Common Criteria test labs or CCTLs. For the United States, the National Voluntary

Laboratory Accreditation Program grants laboratory accreditation and the NIAP CCEVS oversees the CCTLs, which verify a vendor's product security claims using artifacts/proof supplied by the vendor along with the labs' own independent tests. The level of effort and the required vendor proof are based on a scale of assurance levels. Typically, the vendor chooses the evaluation assurance level according to client needs.

An evaluation requires vendors to supply a lab with a set of security claims in the form of a security target, the product to be evaluated, and documentation appropriate for the selected evaluation assurance level. The security target and the evaluation evidence can be developed by the vendor or a hired consultant. Either way, it takes time to prepare the documents adequately.

Once the vendor has supplied the accredited lab with the required materials, the lab conducts the evaluation. If the lab discovers issues during the evaluation, vendors are required to resolve them. The evaluation issue resolution cycle continues until all issues are resolved and the final set of results is submitted to the NIAP CCEVS. Following the NIAP CCEVS validation of the results, the vendor receives a certificate for the particular version and configuration of the product evaluated.

The Driving Forces of Common Criteria

The United States is a leader in the area of CC—in fact, the only country in the world with national regulations requiring CC evaluations. Nineteen other nations currently recognize the importance of the CC and with it the significance of independently certifying the security features and functions in IT products.

NSTISSP #11

NSTISSP #11 took effect in July 2002, and since then, all new IT product purchases for use in national security systems must be evaluated and validated under the Common Criteria. In July 2003, a deferred compliance guidelines annex was added to this policy. The guidelines state that acquisitions made prior to July 2002, are exempt from NSTISSP #11, but those products should be used with care and replaced with validated products as soon as is "practical." The guidelines further state that "no blanket or open-ended waivers . . . will be authorized, but a Deferred Compliance Authorization (DCA) may be granted on a case-by-case basis." The guidelines go on to explain that DCAs are "applicable only to the acquisition of a specific COTS product for a specific application within the IT enterprise of an organization," but they do not "constitute blanket approval for future acquisitions of the same product." Deferrals will be "reviewed and approved only by the heads of federal departments or agencies, or major subordinate organizations within a department or agency."

Directive 8500.1

Following in the footsteps of NSTISSP #11, DoD Directive 8500.1 and DoD Instruction 8500.2 included provisions and guidance for CC evaluations as part of their direction for information assurance within the DoD. Responsibility for ensuring these policies were enforced was also assigned within the policies.

Directive 8500.1 was instituted in October 2002. Its three main tenets state that all IA or IA-enabled products incorporated into DoD information systems must comply with NSTISSP #11; products must be satisfactorily evaluated and validated prior to purchase or as a condition of purchase; and purchase contracts must specify that validation will be maintained for subsequent releases of the product.



**THE DOD MUST
UNDERSTAND THAT CC
EVALUATIONS AND THEIR
SUBSEQUENT MAINTENANCE
ARE NOT TRIVIAL TASKS:
THEY TAKE WEEKS OR
MONTHS TO COMPLETE.**

Of course, the preferred course of action is to have products evaluated prior to purchase, but evaluated products for certain applications are simply not yet available. Fortunately, the “condition of purchase” clause addresses this issue.

This directive places the burden on the heads of DoD components to ensure purchase contracts reflect the proper product evaluation and validation requirements.

Instruction 8500.2

The DoD reinforced Directive 8500.1 and provided instruction on how to execute it in February 2003, with Instruction 8500.2.

There are two key elements to this policy. First, if an approved protection profile (PP)—a statement of security requirements that addresses existing threats in specific technology areas—exists, purchases are restricted to respectively: validated products that match that existing PP; products submitted for validation with a security target written against that PP; or other U.S.-recognized products evaluated under the international Common Criteria Recognition Arrangement (CCRA).

PPs are typically used to let product vendors know what security functionality they must provide to address government and DoD security needs. It is important to note the PP requirements in DoD 8500.2 because the federal government and NSA have identified 10 key technology areas for which they are developing PPs. The areas for which PPs exist or will soon exist are operating systems; firewalls; wireless technologies; Web browsers; intrusion detection devices; databases; public key encryption; biometrics; virtual private networks; and tokens. If a DoD product purchase that falls under DoD 8500.1 fits into one of these technology areas, the DoD procurement officer should be certain his or her vendors work with their chosen CCTL to locate the relevant PP.

If no approved U.S. government PP exists, the acquiring organization must require, prior to purchase, that vendors provide a security target that describes the security attributes of the products. In addition, vendors must also submit their products for evaluation at the appropriate CC assurance level as determined by a DoD information systems security engineer (ISSE) and the appropriate designated approval authority (DAA).

The other key element of Instruction 8500.2 is the inclusion of definitions for generic “robustness” levels and the assignment of “baseline levels” of IA services to those robustness levels, depending on the value of the information and the environment in which the information is used. Robustness level descriptions help the ISSE and DAA determine at which level of CC assurance a product must be evaluated. This information is passed on to the

vendor for use in developing an evaluation services contract with a CCTL.

The ISSE and DAA should also consider the following when selecting the evaluation assurance level: the value of the assets being protected; the risk of those assets being compromised; the resources of those who might try to compromise the assets; and the “robustness requirements, mission, and customer needs.”

Instruction 8500.2 also augments key points from Directive 8500.1. Products available “under multiple-award schedule contracts or non-DoD Government-Wide Acquisition Contracts awarded before July 1, 2002, must be evaluated when and if a version release of the product is made available under the contract.” Simply stated, this means that products that are just now being received by the DoD under contracts awarded before July 1, 2002, must be evaluated and validated under the CC.

The instruction also states that “although products that have not satisfactorily completed evaluation may be used, contracts shall require ... [that] evaluations ... be satisfactorily completed within a specified period of time.” This statement gives contract officers the task of ensuring the purchase contract includes provisions requiring vendors to complete the CC evaluation. Vendors cannot simply submit their products for evaluation and then not complete the process. Vendors can work with their CCTL and the DoD to determine a reasonable period of time for the product evaluation, which could be any number of months depending primarily on product complexity, vendor evidence preparedness, assurance level chosen, and the lab’s familiarity with the technology.

Finally, the instruction states that the original contract must specify that “product validation will be kept current” where use is anticipated for subsequent versions of that product. CC certificate maintenance is another task that requires effort and planning on the part of the vendor because CC certificates apply to a specific version and configuration of a product. The requirements for maintaining that certificate across future versions of the product are described in a document entitled “Assurance Continuity: CCRA Requirements,” issued in February 2004 by the international body responsible for maintaining the Common Criteria. You can obtain a copy of this document from any CCTL or the NIAP CCEVS.

DoD contract officers should ensure their vendors are aware of the evaluation completion and certificate maintenance clauses in their contracts so that products do not fail to meet and maintain the CC certification requirements for continued use within the DoD.

As with Directive 8500.1, the heads of DoD components are entrusted with the responsibilities to ensure DoD in-

formation systems employ solutions in accordance with the DoD 8500.2 sections describing product evaluations.

Public Law 107-314

Further emphasizing the importance the federal government and DoD are placing on product evaluations, public law includes provisions for product evaluations and the often-sought-after waivers to such policy requirements.

Subtitle F: Information Technology, Section 352 of Public Law 107-314, passed in December 2002, directs the secretary of defense to establish a policy to limit the acquisition of information assurance technology products to those products that have been evaluated and validated in accordance with appropriate criteria, schemes, or programs. Such criteria or schemes include the NIAP CCEVS and the internationally developed CC.

While experienced vendors will state that acquisition policy requirements can sometimes be waived, the waiver clause in Public Law 107-314 authorizes the secretary of defense to provide such waivers only for U.S. national security purposes. Therefore, this law makes it difficult to obtain waivers to the DoD acquisition policies requiring CC evaluations.

DoD's Responsibility

Clearly, independent product evaluations are important to both the federal government and the DoD, as NSTISSP #11, DoD 8500.1, DoD 8500.2, and Public Law 107-314 confirm. Such evaluations allow the DoD to have confidence that the products it purchases meet the security claims made by the product vendors. While the bulk of the work for obtaining these evaluations falls to the vendor, the DoD is responsible for ensuring that products are evaluated and validated in accordance with the contract requirements stated in the DoD’s own policies. The DoD is also responsible for assisting the vendor with the selection of the assurance level for the evaluation since that assurance level is chosen based on the information security needs and the application of use within the DoD. The DoD must also understand that such evaluations and their subsequent maintenance are not trivial tasks: They take weeks or months to complete depending on the evaluation assurance level chosen, the preparedness of the vendor to supply the required evidence, and the complexity of the product under evaluation.

Common Criteria evaluations play an important role in protecting DoD information. For this reason, procurement officers, contract officers, and DoD vendors should familiarize themselves with the criteria and the evaluation process.

The author welcomes comments and questions. She can be contacted at malnick@criterianlabs.org.