

## Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) Columbia, Maryland

Robert L. Williamson, Jr., Tammy S. Compton,  
James L. Arnold, Jr., and J. Mark Braga

Technical Directorate, SAIC CCTL,  
Renaissance Center, Columbia, Maryland

“**T**he National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) established a program under the National Information Assurance Partnership (NIAP) to evaluate information technology (IT) product conformance to an international standard. 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. This program has been implemented to help consumers select commercial off-the-shelf IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace.”<sup>1</sup>

Fifteen countries now recognize the Common Criteria (CC) (also known as ISO international standard 15408) as the official third-party evaluation criteria for IT security products. The CC is used in many different applications, from specifying security requirements for IT products and systems, to supporting system-level certification and accreditation processes and acquisitions.

Within the United States, several government and civilian agencies, including the Department of Defense (DoD), require all IT security products used to enter, process, store, display or transmit national security information to be tested against the CC. The DoD requirements are articulated in the National Information Assurance Acquisition Policy-National Security Telecommunications and Information Systems Security Policy No. 11 (NSTISSP-11) (visit: [http://www.nstissc.gov/Assets/pdf/nstissp\\_11.pdf](http://www.nstissc.gov/Assets/pdf/nstissp_11.pdf)).

### History

The Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) was one of the first four U.S. laboratories to be accred-

ited to perform IT evaluations within the CCEVS under the authority of the NIAP. In June 1999, when the NIAP Oversight Board first began accepting applications, the SAIC Trusted Technology Assessment Program (TTAP) Evaluation Facility applied for certification as a CCTL.

The process of accreditation required SAIC to develop a laboratory quality manual defining the organization and operation of the SAIC CCTL. A technical competency examination for laboratory key personnel and a laboratory processes audit were also required.

SAIC was accredited as a CCTL in August 2000 and has maintained its accreditation since that time (see certificate, *Figure 1*). The SAIC CCTL is on the NIAP CCEVS Approved Laboratories list. This accreditation allows the SAIC CCTL staff to evaluate IT products at CC evaluation assurance levels (EAL) 1 through 4.



Figure 1. In August 2000, the SAIC Common Criteria Testing Laboratory (CCTL) was one of the first U.S. laboratories to be approved within the Common Criteria Evaluation and Validation Scheme (CCEVS) for IT Security under the authority of the National Information Assurance Partnership (NIAP)

## FEATURED FACILITY

These assurance levels are recognized through an international reciprocity arrangement. SAIC CCTL staff members have a thorough knowledge of the work contained in the Common Evaluation Methodology (CEM) that is required for international acceptance of all CC evaluations.

SAIC has performed, or currently is performing, evaluations at EAL 2, 3 and 4. Through April 2002, the SAIC CCTL had completed four CC evaluations. Each of these evaluations was subject to CCEVS oversight by government validators.

### Laboratory resources

The most important laboratory resource is the evaluation staff. The SAIC engineers and contractors that make up the CCTL are experienced evaluators. The current CCTL staff is composed of 11 full-time evaluators.

SAIC is a matrix-managed organization with technical experts in every product discipline. From another co-located SAIC division, many system security engineers, with CC evaluation experience, supplement the full-time CCTL staff, as required. Where specialized product knowledge is needed, independent subcontractors are retained.

With more than 45 years of combined commercial product evaluation experience, the SAIC CCTL provides the leadership, management and extensive evaluation experience that have contributed to the laboratory's success as a commercial business. CCTL personnel have a thorough knowledge of the CEM that is required for the successful execution of CC evaluations.

Personnel now employed by the SAIC CCTL influenced the TTAP, the transition program for NIAP, which was the commercial evaluation scheme in effect until the NIAP CCEVS became the U.S. program in 1999. They were key authors of government versions of the CC and related Protection Profile (PP) standards and were members of the committee that defined the TTAP program.

In addition, personnel currently employed by the SAIC CCTL participated in the NSA evaluation program as members of the Technical Review Board (TRB), as the TRB's chief evaluator and as technical evaluation leaders. They have also provided management and technical leadership for the Trusted Product Evaluation Program (TPEP) and the TTAP in subject matter areas relating to operating systems networks, database management systems and network components.

The SAIC CCTL has a well-seasoned working relationship with NIAP management personnel at NSA and NIST. The SAIC CCTL staffers also work well with NIAP personnel who are the technical leads for the NIAP CCEVS program. Many of the NIAP technical leads

have been the SAIC CCTL staff members' colleagues in the resolution of difficult, trusted-technology problems; in TPEP evaluations and oversight; in the development of CC; and in the initial phases of the NIAP program.

### Evaluation projects

The SAIC CCTL has primarily focused on higher assurances and complex products (see *Table 1*).

Before becoming the SAIC CCTL, the SAIC TTAP Evaluation Facility evaluated Microsoft Windows NT 4.0 and Microsoft SQL Server 2000. Both are relatively complex products and were evaluated against the TCSEC C2 evaluation criteria. In contrast, most other products evaluated within the TTAP evaluation paradigm were firewalls at EAL 2.

Since being certified, the SAIC CCTL has continued its trend of targeting complex and higher assurance products to evaluate. The first evaluation conducted by the SAIC CCTL was of a simple hardware switch at EAL 4. In the same timeframe, the SAIC CCTL began working on three operating system evaluation projects: Microsoft Windows 2000, at EAL 4; and SGI IRIX and Trusted IRIX, both at EAL 3.

While the larger operating system projects were underway, the SAIC CCTL evaluated a network content filtering product (Finjan SurfinGate) at EAL 3

<b>SAIC CCTL Evaluation Programs</b>	
<i>SAIC Now in Evaluation</i>	<i>EAL</i>
Microsoft Windows 2000 Professional, Server, and Advanced Server	4
RSA Keon® CA version 6, RSA Keon RA version 6 (Keon is a registered trademark of RSA Security Inc.)	4
Trend Micro InterScan VirusWall for NT v3.52, InterScan VirusWall for Unix/Linux v3.6 version 6	4
Pointsec Mobile Technologies, Inc. Pointsec PC 4.1	4
Netscape Certificate Management System Version 6.1	4
Apple Computer MAC OS X	3
Finjan SurfinShield Corporate Version 5.5	3
NetScreen Security Devices	2
Owl Computing Technologies Inc. Data Diode Version 1.0	2
<i>SAIC NIAP Completed</i>	
Cryptek DiamondTEK Version 2.2	4
Finjan SurfinGate Version 5.6	3
SGI IRIX Version 6.5.13	3
SGI Trusted IRIX/CMW Version 6.5.13	3
<i>SAIC TTAP Completed</i>	
EESI SuperNet 2000 EAL/r1	4
Microsoft Windows NT 4.0 SP6a (TCSEC C2)	3
Microsoft SQL Server 2000	3

*Table 1. The SAIC CCTL has concentrated on complex products such as operating systems at high levels of assurance*

and a virtual private network and firewall product (Cryptek DiamondTEK) at EAL 4.

These products have given the SAIC CCTL substantial experience in the higher commercial assurance levels and also in a variety of product types. The SAIC CCTL now has many additional evaluation projects, including operating systems, network appliances and certificate servers, among others, at assurance levels ranging from EAL 2 to EAL 4 augmented.

### The evaluation criteria

CC version 2.1 is the current version of the CC for an IT evaluation that has mutual international recognition. CC version 2.1 is a set of distinct but related parts that are individual documents. These three parts detail the standard by which laboratories perform their work.

Part 1 of the CC is the general model and the introduction. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.

Part 2 of the CC defines a series of security functional requirements, organized by components, families and classes. These requirements provide a standard way of expressing the specific security functional requirements intended to support organizational security policies and to counter perceived threats to security.

Part 3 of the CC defines a series of assurance security requirements, organized by components, families and classes. These requirements provide a standard way of expressing the specific assurance requirements intended to provide assurance that security functional requirements are properly designed, tested, managed and deployed. Part 3 defines criteria for evaluating PPs and Security Targets. Part 3 also presents predefined packages of assurance in the form of EALs. These EALs are intended to simplify the problem of choosing individual security requirements by predefining discrete levels, each with different assurance objectives.

There are seven hierarchical EAL levels defined in the CC. An accredited commercial CCTL is certified to test security functions from EAL 1 to 4. However with NSA participation, "augmented" evaluations that include security assurance requirements beyond EAL 4, such as those found in EAL 5 through EAL 7, can be conducted.

EAL 1 provides minimal confidence of correct operation. However, it does not provide confidence suitable in an environment that has serious security threats. This assurance level provides review of limited design infor-

mation, independent testing and examination of guidance documentation. An EAL 1 evaluation can be performed at relatively little cost to the developer; however, this assurance level is rarely used due to the lack of assurance gained.

EAL 2 provides low to moderate confidence of correct operation. The added confidence renders EAL 2 products suitable for environments that have some threats to security, though they still must not be too serious. The intent of EAL 2 is that an evaluation should demand no more effort on the part of the developer than good commercial practices. It is believed that EAL 2 might be most applicable to legacy-type security products where a good, complete development record may not be available. This assurance level has been fairly popular with network products (for example, firewalls).

EAL 3 provides moderate confidence of correct operation. The added confidence renders EAL 3 products suitable for environments that have real threats to security, though such products still might have vulnerabilities. The intent of EAL 3 is that the evaluation should require effort on the part of the developer commensurate with conscientious, positive engineering during the design stage. Such an evaluation would include a thorough examination of the target of evaluation and its development and substantial independent testing. In practice, it is possible and perhaps even cost effective to develop evidence and correct development practices after the fact in order to complete an EAL 3 evaluation. This assurance level is claimed to be comparable with the older TCSEC C2 criteria and, as such, is a popular assurance target.

EAL 4 provides moderate to high confidence of correct operation. The added confidence renders EAL 4 products suitable for most commercial environments as well as other environments that have real threats to security. The intent of EAL 4 is that good commercial development practices have been applied. These practices are expected to be rigorous, though they should not necessarily require substantial specialist knowledge, skill or resources. It is expected that EAL 4 is the highest assurance level where it may be economically feasible to retrofit an existing product line in order to complete an evaluation.

EAL 4 is the highest assurance level that CCTLs in the United States are certified to evaluate. EAL 4 is claimed to be comparable to the older TCSEC B1; however this is not a good comparison. TCSEC C2 and TCSEC B1 have essentially the same assurance, the differences being primarily in functional requirements. EAL 4 seems to fit somewhere closer to TCSEC B2 because its design and testing requirements are fairly

close, but EAL 4 does not impose the same level of internal architectural requirements and therefore falls short.

EAL 4 is becoming a popular evaluation target. Developers new to the evaluation business are tending to move toward EAL 3, but those with prior experience are tending to move toward EAL 4. In many cases, EAL 4 is being selected for a marketing advantage or as an equalizer.

EAL 5 through EAL 7 provide substantially more assurance from more formality in design specification, more comprehensive testing and more rigorous development practices. Some requirements at these levels require substantial specialist knowledge, skill and resources. It is generally expected that such evaluations could be increasingly cost prohibitive, though the added assurance should offset the cost. There is very little commercial interest in these assurance packages in the United States; however, DoD is working on at least one assurance package somewhere at EAL 5 to EAL 6.

### The evaluation process

SAIC offers a number of evaluation services that can be broadly grouped into two categories: evaluation preparation and evaluation. SAIC can perform either or both of these activities. In most cases, SAIC has performed both functions to complete an evaluation. However, even in the case where the developer desires to develop (or contract with another organization to develop) its own evidence, SAIC has found it to be effective to assign a vendor advocate to serve as a proactive intermediary between the SAIC CCTL Evaluation Team and the developer. Such an advocate is familiar with the Evaluation Team, can work closely with the developer to ensure there is common understanding and can help mitigate conflicts that might arise. A meeting between the Evaluation Team and a product developer is shown in *Figure 2*.



*Figure 2. Each SAIC CCTL Evaluation Team works closely with the product developer to ensure a common understanding*

Evaluation preparation normally starts with an assessment of the current state of the developer's evaluation evidence. This assessment is valuable because it helps the developer understand the level of effort that will be involved and aids the decision on how to proceed in developing required evidence for the evaluation. If the developer desires to develop its own evidence, SAIC will normally assign an advocate to work with the developer throughout the evaluation to answer questions and to mediate between the developer and the Evaluation Team during the evaluation. However, if the developer desires to have SAIC develop the evidence, a Development Team will be formed to perform the necessary work. Note that the Development Team will be composed of individuals who will *not* work on the Evaluation Team, because this represents an unacceptable conflict of interest for the evaluation.

An SAIC Development Team can create evaluation evidence. The following list summarizes the types of required evaluation evidence:

- **Security Target**—This document defines the intended environment for the evaluated product, as well as the security requirements that must be satisfied. This document is intended to publicly represent the evaluated product and is used by integrators and users when selecting products for their environments.

- **Configuration Management Documentation**—This documentation describes the developer processes to manage the configuration of the product to be evaluated.

- **Product Life-Cycle Documentation**—This documentation describes the processes surrounding the life cycle of the product to be evaluated.

- **Delivery and Operation Documentation**—This documentation describes how the product is distributed to users in a secure manner and how the product can be configured to ensure its security functions when it is received.

- **Design Documentation**—This documentation describes the design of the product to be evaluated. Depending on the assurance level, this documentation will describe the functional interface, high-level design, low-level design and even the implementation of the product.

- **Security Testing Documentation and Tests**—This documentation describes how test coverage has been accomplished. It generally describes both the breadth and depth of testing. Expected and actual testing results are also required. The degree to which the Evaluation Team will ultimately exercise the tests provided by

the developer is dependent on the specific assurance level. In *Figure 3*, staffers perform product testing

■ **Vulnerability Assessment Documentation—**

This documentation explores possible vulnerability and misuse issues of the product. In the case of security functions that are probabilistic in nature, this documentation also provides rationale that the functions are suitable to satisfy the specific assurance goal for the product.



*Figure 3. The evaluation process exercises the security features tests that are provided by the developer*

The specific evidence to be created and the level of effort are dependent on many factors, including developer participation, product complexity and the quality of pre-existing evidence. During the evaluation, the SAIC Development Team remains engaged until the evaluation is completed, initially developing evidence, and later answering issues raised by the SAIC CCTL Evaluation Team.

The Evaluation Team begins its work even before the evaluation begins. Its work includes developing a work plan for the evaluation, detailing the schedule of deliverables and evaluating work packages. The work plan and the Security Target are submitted to the CCEVS. Once the CCEVS accepts the evaluation package, it will assign a validator to oversee the evaluation and schedule a kick-off meeting that will formally start the process.

The first CEM work package is the evaluation of the Security Target. The Security Target is evaluated against the ASE class requirements in Part 3 of the CC, with associated guidance found in the CEM. Because

the Security Target defines the requirements for the product to be evaluated, it must be found to have relatively few problems before evaluation of the product itself can begin.

Once the Security Target has been evaluated, and the Evaluation Team believes it is adequate to represent the requirements for the product, evaluation of the product begins. In general, the evaluation will proceed with the evidence that is ready when the evaluation begins.

Typically, evidence is being created in parallel with the evaluation. Configuration management, life cycle, guidance documentation, and delivery and operation documentation have few if any dependencies on other evidence and can usually be added at any time during the evaluation.

However, there may be cases when these documents need to be revisited even after being evaluated. Some evidence is interdependent and must be addressed using an iterative process. For example, the functional interface specification might imply functions that are not covered in an administrator guide. In this case, it does not help to evaluate the functional specification first, because the administrator guide might also imply functions missing from the interface specification.

Still other evaluation evidence is strongly dependent on other evidence.

Evaluation of testing and vulnerability analysis materials can only effectively be accomplished after the design documentation has been evaluated, because these materials serve to provide coverage for the functions described in the design. Evaluating evidence in an inappropriate order can cause significant unnecessary rework.

Throughout the evaluation, the Evaluation Team prepares Evaluation Technical Reports (ETRs) that document the results of performing the work units described in the CEM. These ETRs are used to communicate problems to the developer and also to demonstrate to the CCEVS, via the validator, that the required evaluation work units have been properly performed. Ultimately, the validator must review and accept all of the ETRs before the evaluation can conclude.

Once the ETRs demonstrate that all of the CEM evaluation work units have been performed, and the results are positive, the validator writes a validation report and makes a recommendation to the CCEVS. Subsequently, the CCEVS accepts the validator recommendation and issues a certificate for the evaluat-



Figure 4. Successful evaluation certificates are visible to visitors entering the SAIC CCTL facility

ed product. These certificates are on display in the CCTL facility (Figure 4). The CCEVS also posts information about the evaluation, in the form of the Security Target and Validator Report, on its Validated Product List at [niap.nist.gov/cc-scheme/ValidatedProducts.html](http://niap.nist.gov/cc-scheme/ValidatedProducts.html).

### Facilities

The SAIC CCTL facilities, located at 7125 Columbia Gateway Drive, Suite 300, Columbia, Maryland, have controlled access. All server and telephony rooms, laboratory spaces (with cipher locks) and offices are individual-

ly locked to provide additional physical protection. Each office can be used as an isolated and controlled laboratory environment (Figure 5) where developer-provided hardware and software is installed to support evaluation testing.

CCTL-designated facilities have SAIC-provided Internet connectivity for e-mail, web browsing and ftp. However, access is controlled to minimize the risk of exposure to malicious code and to protect the SAIC network from external tampering or access. Microsoft Visual SourceSafe running on a dedicated CCTL server provides controlled, secure access to proprietary documents.

Within the CCTL facilities, there are dedicated laboratory networks, only some of which have connections to the Internet. Effectively, the CCTL has the equipment necessary to construct a number of simultaneous dedicated and isolated local area networks (LANs) as needed to meet evaluation demands.

SAIC employees in other company locations, as well as subcontract employees, are sometimes required to perform testing assignments at the Columbia CCTL facility. These individuals are supplied with CCTL workstations that have Internet access and desktop publishing tools. Their workstations are part of a Windows NT domain established by the SAIC CCTL. User accounts within this domain are employed to enforce access control on the file server used for testing. □



Figure 5. Offices are utilized as isolated and controlled laboratory environments where developer-provided hardware and software support the Common Criteria (CC) testing effort

### Endnote

<sup>1</sup> Source: National Information Assurance Partnership (NIAP) web page, <http://niap.nist.gov/niap/projects/cc-scheme.html>

### To contact the CCTL:

Customers and government organizations can obtain more information about SAIC CCTL products and services by visiting the web site at [www.saic.com/securebiz](http://www.saic.com/securebiz), e-mailing [robert.l.williamson@saic.com](mailto:robert.l.williamson@saic.com), or calling the laboratory at (410) 953-6819.

### Acknowledgments

Some Common Criteria (CC) descriptive material for this article was taken from existing National Information Assurance Partnership (NIAP) and CC documents and web sites.