



Common Criteria Evaluation and Validation Scheme

Publication #1

Organization, Management and Concept of Operations

8 September 2008
Version 2.0

Foreword

The Common Criteria Evaluation and Validation Scheme (CCEVS) was established to ensure the ready availability of independently evaluated and validated IT products that meet the security needs of the United States Government.

Audrey M. Dale
Director, CCEVS

All correspondence in connection with this document should be addressed to:

National Security Agency
Common Criteria Evaluation and Validation Scheme
9800 Savage Road, Suite 6757
Fort George G. Meade, MD 20755-6757
E-mail: scheme-comments@missi.ncsc.mil
<http://www.niap-ccevs.org/cc-scheme>

Amendment record

Version	Date	Description
2.0	May 1999	Initial release.
2.0	8 September 2008	Complete revision based on current operations. The version number remained 2.0 to be consistent across all publications updated in 2008.

(This page intentionally left blank)

Table of Contents

1	Introduction	1
1.1	Objectives.....	1
1.2	IT Security Evaluation and Validation.....	2
1.3	Historical Perspective.....	3
1.4	Purpose and Organization of this Document.....	4
1.5	Scheme Publications	4
2	Overview of the Scheme.....	5
3	Roles and Responsibilities.....	8
3.1	Sponsor of an IT Security Evaluation	8
3.2	CCEVS	8
3.3	Common Criteria Testing Laboratories.....	10
3.4	Guidance for Consumers	12
4	IT Security Evaluation and Validation.....	13
4.1	Preparation for IT Security Evaluation	13
4.1.1	Consultancy Work in Support of Evaluations.....	13
4.1.2	Security Target	13
4.1.3	Deliverables.....	14
4.1.4	Readiness for Evaluation.....	14
4.2	Technical Oversight	15
4.2.1	CCTL Accreditation and Monitoring.....	15
4.2.2	Scope of Technical Oversight	15
4.3	Conduct of the IT Security Evaluation and Validation	16
4.3.1	Entering the Scheme.....	16
4.3.2	Evaluation Activities	17
4.3.3	The Validation Oversight Review (VOR) Process	18
4.4	Conclusion of the Evaluation	18
4.5	Evaluation of Protection Profiles	19
5	Common Criteria Certificates.....	20
5.1	Proper Use of CC Certificate	20
5.2	Certificate Maintenance	20
	Annex A: References.....	21
	Annex B: Acronyms.....	22
	Annex C: Glossary	24
	Annex D: Common Criteria Certificates.....	27

1 Introduction

Since the 1980s, advances in information technologies and the proliferation of computing systems and networks worldwide have raised the level of concern over security in both the public and private sectors. This concern was reinforced in the final report of the President's Commission on Critical Infrastructure Protection and the associated Presidential Decision Directive 63 (PDD-63) published in 1998 and has continued to multiply into the 2000s.

Security concerns are motivated by an increasing use of Information Assurance (IA) and IA-Enabled information technology (IT) products and systems throughout government and industry in a variety of areas from electronic commerce to national defense. Consumers have access to a growing number of security-enhanced IT products with different capabilities and limitations and must make important decisions about which products provide an appropriate degree of protection for their information.

In order to help consumers select commercial off-the-shelf (COTS) Information Assurance (IA) and IA-Enabled IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace, the National Security Agency (NSA) manages and maintains a program to evaluate Information Assurance (IA) and IA-Enabled IT product conformance to international standards. This program is called the Common Criteria Evaluation and Validation Scheme, (CCEVS) - also referred to throughout this document as the Common Criteria Scheme or just the Scheme.

1.1 Objectives

The primary objectives of the CCEVS are to:

- a. meet the needs of government and industry for cost-effective evaluations of IT products;
- b. encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry;
- c. ensure that security evaluations of IT products are performed to consistent standards;
- d. improve the availability of evaluated IT products.

The CCEVS serves many communities of interest with very diverse roles and responsibilities. These communities include IT product developers, product vendors, value-added resellers, systems integrators, IT security researchers, acquisition/procurement authorities, consumers of IT products, auditors, and system accreditors. Close cooperation between government and industry is paramount to the success of the scheme and the realization of its objectives.

1.2 IT Security Evaluation and Validation

IT security is defined as the protection of information from unauthorized disclosure, modification, or loss of use by countering threats to that information arising from human or systems-generated activities, malicious or otherwise. Countering threats to an IT product and mitigating risk helps to protect the confidentiality and integrity of information and to ensure its availability.

Consumers of IT products need to have confidence in the security features of those products. Consumers want to be able to compare various products to understand their capabilities and limitations. Confidence in a particular IT product can be based on the trusted reputation of the developer, past experience in dealing with the developer, or the demonstrated competence of the developer in building products through recognized assessments. The consumer could also test the product directly and obtain the necessary results. The first approach lacks measurable results and the second approach requires substantial, costly duplication of effort.

The Common Criteria Scheme overcomes these limitations and enables consumers to obtain an impartial assessment of an IT product by an independent entity. This impartial assessment, or security evaluation, includes an analysis of the IT product and the testing of the product for conformance to a set of security requirements. The IT product being evaluated is referred to as the Target of Evaluation (TOE). The security requirements for that product are described in its security target. IT security evaluations are composed of analysis and testing, distinguishing these activities from the more traditional forms of conformance testing in other areas.

It is important that security evaluations of IT products be carried out in accordance with recognized standards and procedures. The use of standard IT security evaluation criteria and IT security evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgment and background knowledge for which consistency is more difficult to achieve.

To increase the consumer's level of confidence in IT security evaluations, the final evaluation results are reviewed by an independent party. This review provides independent confirmation that an IT security evaluation was conducted in accordance with the provisions of the scheme and that the conclusions of the testing laboratory are consistent with the facts presented in the evaluation. This review, known as validation, is intended to promote consistency of IT security evaluations and comparability of results for all evaluations conducted within the scheme.

The impartial evaluation, the independent validation of evaluation results, and the documentation resulting from these processes provide valuable information for consumers about the security capability of IT products. However, consumers will still need to review this information carefully and assess its applicability to local needs, (e.g., the situation and operating environment in which the product will actually be used).

Section 3.4 of this document provides additional guidance to consumers of IT products regarding the specific use of security evaluation results.

Participation in the scheme and its associated evaluation and validation activities is strictly voluntary (unless mandated by government policy or regulation). A more complete description of these testing and evaluation activities and how these activities relate to the scheme can be found in [Publication #4](#) *Guidance to Common Criteria Testing Laboratories*.

1.3 Historical Perspective

The U.S. Government supports the security and trustworthiness of IT products that are part of the national information infrastructure, both in the public and private sectors. In fulfilling their responsibilities under Public Law 100-235 (Computer Security Act of 1987), both the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have worked with government and industry to develop and apply information security technology, assurance metrics and standards necessary for the protection of information critical to the overall economic and national security interests of the United States.

For over two decades, beginning in the 1980s, NIST and NSA promoted security in commercial off-the-shelf IT products. These efforts focused primarily on government-sponsored initiatives to produce effective IT security evaluation criteria, (e.g., the Trusted Computer System Evaluation Criteria [DOD85] and the Federal Criteria for Information Technology Security [FED92]), and to evaluate products developed by industry in response to those criteria. The development of similar IT security evaluation criteria by Canada and several European nations and recognition of the increasing world wide markets for U.S. manufacturers of IT products prompted the effort to begin harmonizing existing evaluation criteria into common criteria—internationally accepted and standards-based. The Common Criteria was established in 1997 as the result of a multi-year effort by the governments of the U.S., Canada, United Kingdom, France, Germany, and the Netherlands to develop harmonized security criteria for IT products. In 1998, version 2.1 of the CC was accepted by the International Organization for Standardization (ISO) as ISO standard 15408.

At the same time the Common Criteria was being developed, there was a parallel effort to transition trusted product evaluations from the government to the private sector. NSA began the transition of its commercial IT product evaluation capability, (i.e., the Trusted Product Evaluation Program) to the private sector with the establishment of the Trust Technology Assessment Program (TTAP). Under this program, IT security evaluations were conducted by commercial testing laboratories using the NSA evaluation methodology in accordance with cooperative research and development agreements. The transition continued under the Common Criteria Evaluation and Validation Scheme (CCEVS) with commercial testing laboratories conducting Common Criteria-based evaluations of Information Assurance (IA) and IA-Enabled IT products on a fee-for-service basis using the Common Evaluation Methodology.

The Common Criteria Scheme has grown substantially since its inception in 2000 from managing just a few accredited commercial testing laboratories and having a handful of products in evaluation to overseeing eight Common Criteria Testing Labs (CCTLs) with over 100 products in evaluation and successfully completing nearly 300 evaluations.

1.4 Purpose and Organization of this Document

This document is intended to provide a high level overview and description of the Common Criteria Evaluation and Validation Scheme to all interested parties including sponsors, vendors, CCTLs and consumers of evaluated products. It consists of five chapters and several supporting annexes. Chapter 1 introduces the concept of an evaluation and validation scheme and provides a historical perspective on the establishment of the scheme, chapter 2 provides a general overview of the scheme and a brief description of its major activities, chapter 3 defines the roles and responsibilities of the key participants in the scheme to include the CCEVS, CCTLs, and sponsors of IT security evaluations, chapter 4 describes the activities associated with conducting IT security evaluations, and chapter 5 elaborates on the concept of technical oversight and validation and describes the interaction between the CCEVS and security testing laboratories. The annexes include an acronym list, a glossary, a list of references, and a description and example of a Common Criteria Certificate.

1.5 Scheme Publications

The CCEVS communicates to sponsors of evaluations, testing laboratories, government agencies, and the general public through a variety of documents to include the following publications:

[Publication #1](#), *Common Criteria Evaluation and Validation Scheme -- Organization, Management, and Concept of Operations*

[Publication #2](#), *Common Criteria Evaluation and Validation Scheme – Quality Manual and Standard Operating Procedures*

[Publication #3](#), *Common Criteria Evaluation and Validation Scheme -- Guidance to Validators*

[Publication #4](#), *Common Criteria Evaluation and Validation Scheme -- Guidance to Common Criteria Testing Laboratories*

[Publication #5](#), *Common Criteria Evaluation and Validation Scheme -- Guidance to Sponsors*

[Publication #6](#), *Common Criteria Evaluation and Validation Scheme – Assurance Continuity: Guidance for Maintenance and Re-evaluation*

These publications along with additional information, documents and guidance is available on the CCEVS web site at <http://www.niap-ccevs.org/cc-scheme>

2 Overview of the Scheme

This chapter provides a general overview of the Common Criteria Scheme. The principal participants in the scheme are the:

- **Sponsor:** The Sponsor may be a product developer, a Protection Profile developer, a value-added reseller of an IT security-enabled product, or another party that wishes to have a product or PP evaluated. The sponsor requests that a Common Criteria Testing Laboratory (CCTL) conduct a security evaluation of an IT product or PP.
- **Common Criteria Testing Laboratory (CCTL):** The CCTL is a commercial testing laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS to perform security evaluations against the *Common Criteria for Information Technology Security Evaluation (CC)* using the *Common Methodology for Information Technology Security Evaluation (CEM)*.
- **Common Criteria Evaluation and Validation Scheme (CCEVS):** The CCEVS is the government organization established to maintain and operate the scheme for the U.S. Government and to oversee and validate the evaluations performed by the CCTLs.

In addition to the principal participants listed above, the NIST *National Voluntary Laboratory Accreditation Program (NVLAP)* plays an important role in supporting the scheme requirements for laboratory accreditation.

In the context of the Common Criteria Scheme, a sponsor is the party requesting and paying for the security evaluation of an IT product or *protection profile*¹ by an accredited testing laboratory. The sponsor is often the product or profile developer, but could also be a government agency, industry consortium, or other organization seeking to obtain an IT security evaluation.

The CCEVS is the organization managed by NSA and staffed by technical/administrative personnel. Operating in the interest of the public and private sectors, the CCEVS approves participation of security testing laboratories in the scheme in accordance with its established policies and procedures. It also provides technical guidance to those

¹A protection profile is a Common Criteria construct that defines an implementation-independent set of IT security requirements (both features and assurances) for a category of IT products. Such generalized requirements are intended to meet common needs for IT security. Consumers can therefore, construct or cite a protection profile to express their IT security needs without reference to any specific IT product. Sponsors may employ CCTLs to formally evaluate protection profiles in accordance with the Common Criteria and the Common Methodology. The results of such evaluations can be validated by the CCEVS and appropriate Common Criteria certificates issued. Protection profiles can subsequently be listed in a special section of the validated products list.

testing laboratories, validates the results of IT security evaluations for conformance to the Common Criteria, and serves as an interface to other nations on the mutual recognition of such evaluations.

IT security evaluations are conducted by commercial testing laboratories accredited by the National Voluntary Lab Accreditation Program (NVLAP) and approved by the CCEVS . These approved testing laboratories are called Common Criteria Testing Laboratories (CCTLs). NVLAP accreditation is the primary requirement for becoming a CCTL.² The purpose of the NVLAP accreditation is to ensure that laboratories meet the requirements of ISO/IEC Guide 25, *General Requirements for the Competence of Calibration and Testing Laboratories* and the specific scheme requirements for IT security evaluations.

With respect to NVLAP, the scope of accreditation is defined to be the particular *test methods*³ that a laboratory will use in conducting IT security evaluations. A testing laboratory will choose its scope of accreditation from a list of approved test methods developed by the CCEVS. The CCEVS maintains a *CCEVS Approved Test Methods List* for use by a laboratory in selecting its proposed scope of accreditation. The CCEVS coordinates with NVLAP to ensure the appropriate accreditation is made available to CCTLs. Once NVLAP accreditation is received and any additional scheme-specific requirements are met, the CCTL is placed on the *CCEVS Approved Laboratories List*.

CCTLs wishing to expand their scope of accreditation, (i.e., adding new test methods), will coordinate with NVLAP and CCEVS. Specific details regarding NVLAP accreditation, re-accreditation, expansion of scope, and the testing laboratory approval process can be found in Pub #4 *Guidance to CCEVS Approved Common Criteria Testing Laboratories*.

The CCEVS validates the results of a security evaluation conducted by a CCTL within the scheme and, when appropriate, issues a Common Criteria certificate. The certificate, together with its associated validation report, confirms that an IT product or protection profile has been evaluated at an accredited testing laboratory using the Common Methodology for conformance to the Common Criteria. The certificate also confirms that the IT security evaluation has been conducted in accordance with the provisions of the scheme and that the conclusions of the testing laboratory are consistent with the evidence presented during the evaluation.

The CCEVS maintains a *Validated Products List* containing all Information Assurance (IA) and IA-Enabled IT products and protection profiles that have successfully completed

²There are scheme requirements in addition to NVLAP accreditation that are handled by the CCEVS as part of the overall laboratory approval process. These additional requirements are described in Scheme Publication #2, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—CCEVS Quality Manual and Standard Operating Procedures*.

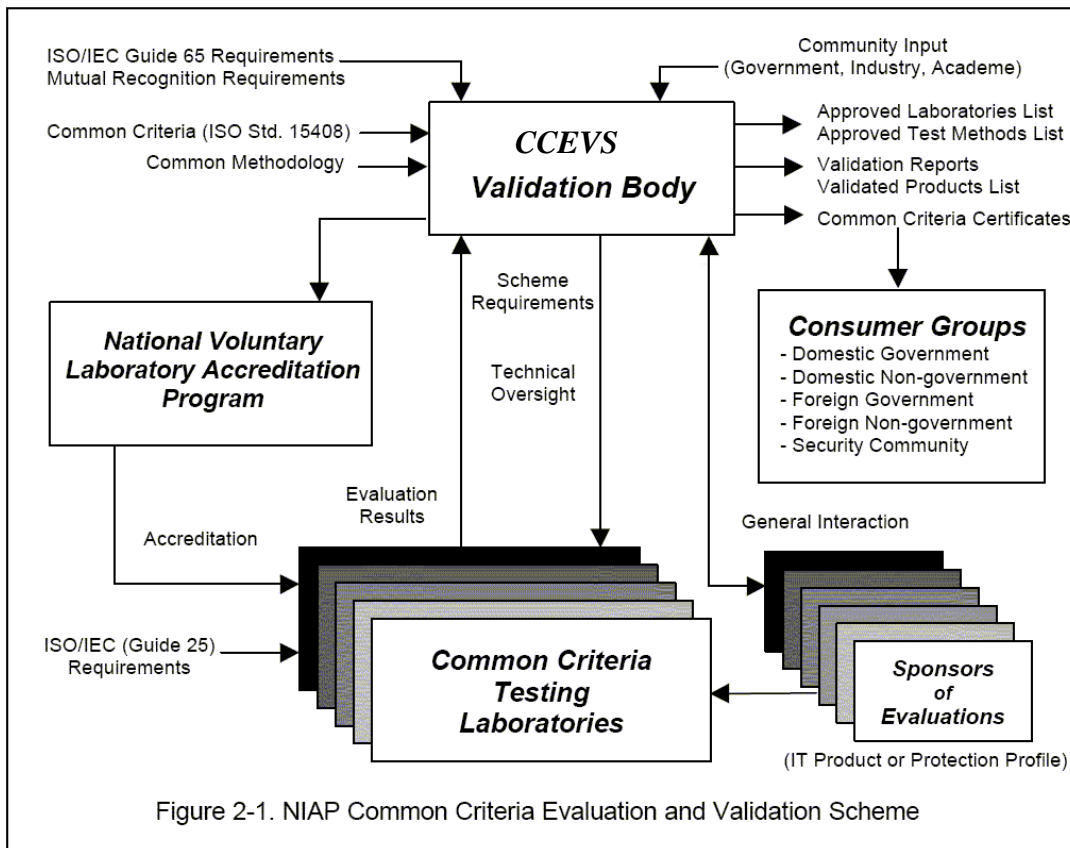
³ In the scheme, a test method is defined to be a Common Criteria assurance package and the associated evaluation methodology for that assurance package from the Common Methodology. Initially, the scheme will provide a limited number of test methods, primarily corresponding to the Common Criteria Evaluation Assurance Levels (EALs) 1 through 4 and the associated evaluation methodology for those EALs. Test methods for protection profile and security target evaluations will also be offered. Additional test methods may be subsequently defined based on consumer requirements, technical viability, and scheme experience.

evaluation and validation under the scheme. In addition, CCEVS also maintains a list of products that are in the evaluation process. These lists are located on the CCEVS web site at <http://www.niap-ccevs.org/cc-scheme/>.

In order for IT products to receive Common Criteria certificates and be placed on the CCEVS *Validated Products List*, evaluations must be performed against explicit security targets. A security target may or may not claim conformance to a protection profile. A security target claiming conformance to a particular protection profile must be evaluated against that profile to substantiate the claim. This evaluation is conducted in addition to, and in conjunction with, the evaluation of the actual IT product against its security target.

The cost of an IT security evaluation will be determined strictly by the individual contract negotiations between the sponsor of the evaluation and testing laboratory selected to conduct the evaluation. The CCEVS does not play a role in sponsor-laboratory contract negotiations. Since the inception of the program, CCEVS has not charged sponsors for validation services but is, however, pursuing a cost recovery program for validation services in the future.

Figure 2-1 illustrates the relationships among key participants within the Common Criteria Scheme.



3 Roles and Responsibilities

This chapter describes the roles and responsibilities of the principal participants in the Common Criteria Scheme, (i.e., sponsors of IT security evaluations, the CCEVS, and Common Criteria Testing Laboratories).

3.1 Sponsor of an IT Security Evaluation

The *sponsor* is the individual or organization requesting a security evaluation of an IT product or a protection profile. The relationship of the sponsor to the IT product or protection profile may vary depending on the nature of the product or profile and the circumstances surrounding the evaluation. In most cases, the sponsor of a security evaluation will be the actual developer of the IT product or protection profile. However, this may not always be the case. The sponsor of a security evaluation may be a value-added reseller of an IT product or an organization or individual involved in the acquisition of an IT system that includes that particular product as a key component.

In cases where the sponsor of an evaluation is not the developer of the product or protection profile, the sponsor needs to obtain the cooperation of the developer in providing the CCTL with technical materials and essential deliverables necessary to conduct the IT security evaluation in a complete and consistent manner. The specific details of the provision of documentation for the security evaluation will be handled in contractual agreements between the sponsor and the IT product or protection profile developer. The specific obligations of the sponsor of an evaluation are outlined in Pub #5 *Guidance to Sponsors of IT Security Evaluations*.

3.2 CCEVS

The principal objective of the CCEVS is to ensure the provision of competent IT security evaluation and validation services for both government and industry. The CCEVS has the ultimate responsibility for the operation of the scheme in accordance with its policies and procedures and, where appropriate, for the interpretation and amendment of those policies and procedures. NSA is responsible for providing sufficient resources to the CCEVS to carry out its responsibilities.

The CCEVS must ensure that appropriate mechanisms are in place to protect the interests of all parties within the scheme participating in the process of IT security evaluation. Any dispute brought forth by a participating party, (i.e., sponsor of an evaluation, product or protection profile developer, or CCTL), concerning the operation of the scheme or any of its associated activities shall be referred to the CCEVS for resolution.

The CCEVS is led by a Director selected by NSA management. The Director of the CCEVS reports to the Information Assurance Director, (IAD/NSA), or their designated representative, for administrative and budgetary matters and is responsible for scheme-related operational matters. There are also technical and administrative support personnel required to provide a full range of validation services for the sponsors of evaluations and the CCTLs. These personnel include validators, technical experts, and senior members of

the technical staff. For additional details, see [Publication #2 Quality Manual and Standard Operating Procedures](#).

In general, the responsibilities of the CCEVS are:

- a) to establish and implement policies and procedures for the operation of the scheme, and to ensure that these policies and procedures are adhered to;
- b) to document and publicize the organization, policies, and procedures of the scheme;
- c) to approve CCTL participation in the scheme and publicize the approved CCTLs on the CCEVS Approved Laboratories List;
- d) to monitor the performance of participating CCTLs and their adherence to, application of and interpretation of the Common Criteria and the Common Methodology;
- e) to remove a CCTL from the CCEVS Approved Laboratories List if the laboratory fails to meet the terms and conditions of the scheme;
- f) to provide notice to the community of any changes to the CCEVS Approved Laboratories List including additions or withdrawals of CCTLs from the scheme and any modifications to the scope of a laboratory's accreditation;
- g) to ensure that appropriate procedures are in place within the scheme to protect sensitive or proprietary information relating to IT products or protection profiles under evaluation and that those procedures are routinely followed;
- h) to provide advice, guidance, support, and standards for training to CCTLs as required;
- i) to review evaluation technical reports from CCTLs to ensure that the conclusions are consistent with the evidence presented and that the Common Criteria and the Common Methodology have been correctly applied;
- j) to ensure consistency of CCTL evaluations across the scheme;
- k) to seek guidance from industry experts, (e.g., consumer groups, IT product or protection profile developers, testing laboratories, researchers, standards groups), when resolving disputes, addressing challenges, answering technical questions or making critical decisions regarding any aspect of the scheme;
- l) to issue Common Criteria certificates for products or protection profiles successfully evaluated and validated by the scheme

- m) to publish and maintain a validated products list of all successfully evaluated and validated products or protection profiles, along with their respective security targets/protection profiles and validation reports;
- n) to promote the integrity of the Common Criteria certificates and ensure the Common Criteria and CCEVS logos are used correctly;
- o) to ensure that the interests of all parties participating in scheme activities are given appropriate consideration;
- p) to arbitrate disputes arising in the context of the scheme and provide procedures for appeal or reconciliation;
- q) to approve press releases or similar statements relating to the scheme; and
- r) to maintain a record system for creating, storing, accessing, archiving and disposing of scheme records used to document CCEVS activities.

Specific requirements for the CCEVS are outlined in [Publication #2](#) *Quality Manual and Standard Operating Procedures*.

In order to carry out its scheme responsibilities and fulfill the conditions of the Agreement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security, the CCEVS must maintain a high degree of technical expertise and competence in all aspects of security testing and evaluation. This expertise is critical to conducting validations and providing the necessary technical support to sponsors of evaluations and to CCTLs participating in the scheme. To that end, the CCEVS reserves the right to place its technical personnel in selected CCTLs for the express purpose of observing and/or participating in Common Criteria-based evaluations in a variety of technology areas.

3.3 Common Criteria Testing Laboratories

CCTLs are testing laboratories that are accredited by NVLAP and listed on an approved laboratories list by the CCEVS. These laboratories must meet the requirements of:

- a) [NIST Handbook 150:2005](#), *Procedures and General Requirements*;⁴
- b) [NIST Handbook 150-20](#), *Information Technology Security Testing—Common Criteria*;

⁴NIST Handbook 150 contains the requirements of ISO/IEC Guide 25, *General Requirements for the Competence of Calibration and Testing Laboratories*. ISO/IEC Technical Report 13233, *Information Technology-Interpretation of Accreditation Requirements in Guide 25 Accreditation of Information Technology and Telecommunications Testing Laboratories for Software and Protocol Testing Services* is used by NVLAP to interpret the requirements of ISO/IEC Guide 25 for CCTLs.

- c) Specific criteria for IT security evaluations and other requirements of the scheme as defined by the CCEVS (see Pub #4 *Guidance to CCEVS Approved Common Criteria Testing Laboratories*).

CCTLs enter into contractual agreements with sponsors to conduct security evaluations⁵ of IT products and protection profiles using CCEVS-approved test methods derived from the Common Criteria, Common Methodology and other technology-based sources. The IT security evaluations are carried out in accordance with the policies and procedures of the scheme.

CCTLs must observe the highest standards of impartiality, integrity, and commercial confidentiality, and operate within the guidelines established by the scheme. With respect to commercial confidentiality, CCTLs must have documented policy and procedures to ensure the protection of sensitive or proprietary information. These procedures shall be subject to audit by NVLAP and the CCEVS.

In order to avoid any actual or potential conflict of interest, the CCTL must agree that they will not accept for evaluation any product developed, manufactured, or sold by an entity that possesses an ownership interest in the CCTL or in which the CCTL has an ownership interest. Within the context of this policy, the term “ownership interest” shall include any percentage of ownership which is greater than 5%. Other prohibited relationships include, but are not limited to, situations in which the CCTL has entered into an agreement that would result in the CCTL directly benefiting financially from commercial sales of the product being evaluated or in which the CCTL has sole distributorship for the evaluated product.

Neither the CCTL, nor any individual CCTL staff members concerned with a particular IT security evaluation, may have a vested interest in the outcome of that evaluation. A CCTL staff member or evaluation team cannot, under any circumstances, be involved in:

- a) both the development and the evaluation of an IT product or protection profile;
- b) the provision of consultancy services to the sponsor of an evaluation or a product/profile developer which would compromise the independence of the evaluation.

Accordingly, CCTLs must ensure that any activities related to the production of evaluation evidence for a particular IT product or protection profile preparing to enter evaluation (within that same testing laboratory) do not conflict with the laboratory’s ability to conduct a fair and impartial evaluation of that product or profile. The above conflict of interest guidelines will be subject to the scrutiny of the CCEVS and NVLAP to ensure these conditions are met. The CCEVS and NVLAP will be the final arbiters in

⁵ The purpose of a security evaluation is to confirm that an IT product meets its security target. To accomplish this, CCTL evaluators must understand the product, its security policy, and how the security features enforce the product’s security policy. Evaluators must also test the security features of the product and write a final evaluation technical report describing their analysis and testing.

determining potential or actual conflicts of interest which may threaten the integrity of security evaluations conducted within the scheme.

A CCTL shall provide the CCEVS with thirty days notice of its intention to withdraw from the scheme. Additional laboratory-related information can be found in [Publication #4 Guidance to Common Criteria Testing Laboratories](#).

3.4 Guidance for Consumers

It is important that consumers of IT products and protection profiles understand how to interpret the results of IT security evaluations conducted within the scheme. These results are described in evaluation technical reports produced by the CCTLs and summarized in the associated validation reports and Common Criteria certificates published by the CCEVS.

An IT product is typically evaluated in a generic laboratory setting at a CCTL within the scheme. In that regard, there are some general assumptions made about the operational environment where the product will ultimately be deployed once the evaluation has been completed.. In some cases, an evaluated IT product may be integrated into a more complex configuration of products that compose an IT system. The actual environment may also be significantly different from the one described in the original assumptions set forth in the security target. In the end, consumers must assess the overall contribution to assurance made by the evaluated IT product. When making that assessment, there are several things a consumer should consider:

- a) The accuracy and completeness of security evaluation results are dependent on the accuracy and completeness of the information and documentation provided to the CCTL by the sponsor of the evaluation;
- b) The quality of a security target, (i.e., security specification), and the reported results of an IT product evaluated against that security target, are a function of how well the product is able to be described under the Common Criteria and the degree to which the Common Methodology and the derivative test methods are able to measure conformance to the security target;
- c) The security evaluation results are only applicable to that particular version and release of the product in its evaluated configuration. Consumers are responsible for determining the security impact of installing or operating an evaluated IT product in a configuration other than the configuration in which it was evaluated.

4 IT Security Evaluation and Validation

This chapter describes the activities of the Common Criteria Scheme participants during the various stages of an IT security evaluation.⁶

4.1 Preparation for IT Security Evaluation

The majority of activity in the early stages of an evaluation takes place between the sponsor of the evaluation and CCTL. The sponsor is responsible for providing the security target and the associated IT product that will become the Target of Evaluation (TOE). The composition of a TOE may be varied and consist of hardware, firmware, and software (or any combination thereof). The TOE may also include multiple IT products (sometimes referred to as an IT system), some of which may already be evaluated. All security-relevant information and documentation produced during the IT product development process shall be included in the deliverables supplied to the CCTL conducting the evaluation. The sponsor must ensure that arrangements have been made to provide all essential documentation to the CCTL in order to conduct a successful security evaluation.

4.1.1 Consultancy Work in Support of Evaluations

Common Criteria evaluation consultants may be hired to assist the sponsor in preparing for an evaluation (e.g., reviewing and preparing evaluation evidence, assisting in resolving evaluation issues, etc.) Hiring an evaluation consultant is not required, nor is CCEVS involved in this decision. Consultants may work for a CCTL, or be independently employed. The decision of whether to hire a consultant and who to hire for consultancy work will be left solely to the sponsor. The scope of consultancy work during the preparation for an IT security evaluation is not controlled by the scheme and is a matter for negotiation between the sponsor and the consultant. However, if the CCTL is used for consultancy, it must adhere to the terms and conditions of its NVLAP accreditation and CCEVS conflict of interest guidelines to ensure that the advice given does not affect evaluator independence or impartiality in any evaluation.

For each evaluation, CCTLs shall notify the CCEVS of any consultancy activities conducted on behalf of a sponsor of an evaluation that are relevant to that evaluation. These activities must not inhibit the CCTL from demonstrating that its independence and impartiality will be maintained during the evaluation.

4.1.2 Security Target

The security target serves as both a specification of the security functions against which the IT product, (i.e., TOE), will be evaluated and as a description relating the product to the environment in which it will operate. The sponsor of an evaluation provides the security target, which includes a list of claims about the IT product made by the sponsor. The content and presentation of the security target must be specified in terms of the Common Criteria. The security target may also claim conformance to a protection profile.

⁶This chapter focuses primarily on the evaluation of IT products. Therefore, some of the information is not applicable to the evaluation of protection profiles. Section 4.4 provides additional information regarding protection profile evaluations.

4.1.3 Deliverables

The deliverables for an IT security evaluation are typically items of hardware, firmware, software or other technical documentation normally generated during the development of the product. The sponsor of an evaluation must ensure the timely supply of deliverables for the evaluation. Appropriate contractual arrangements shall be made by the sponsor to ensure the supply of evaluation deliverables to the CCTL. If the TOE consists of multiple IT products, some of which have been previously evaluated, the sponsor of the evaluation must ensure that contractual arrangements include authority for the release of previous evaluation results.

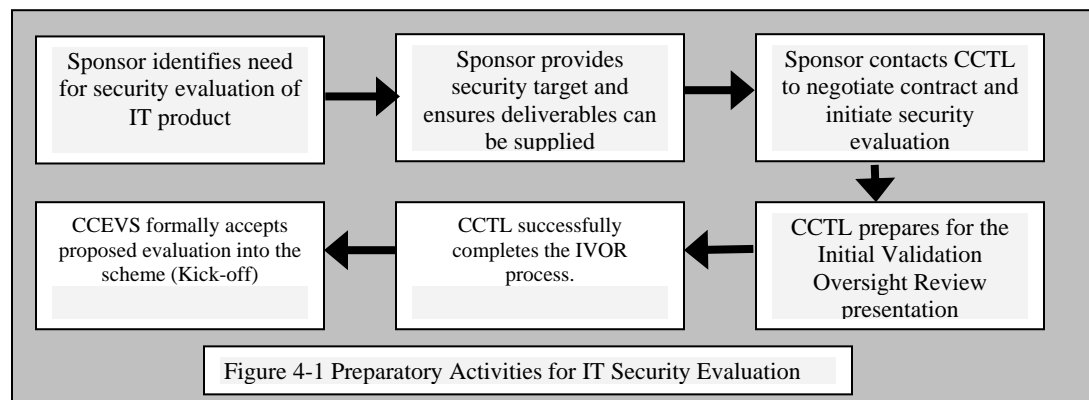
The sponsor of an IT security evaluation must ensure that the CCTL and the CCEVS have access to any proprietary information necessary to conduct the evaluation and validation, respectively. The CCTL may be unable to perform an evaluation of the product and the CCEVS may be unable to publish its validation report if access to such proprietary information is denied.

The CCEVS and CCTL shall ensure that no sensitive or proprietary information is released to unauthorized parties during the course of an evaluation. The CCTL shall ensure that the nature and extent of the proprietary information is defined and apply appropriate rules for its protection.

4.1.4 Readiness for Evaluation

Once the sponsor has established the security target and the strategy for the supply of deliverables, the sponsor should approach a CCTL to initiate the evaluation of the product. A sponsor may also use the completed security target to obtain evaluation proposals from CCTLs.

The CCTL selected to conduct the evaluation should review the security target to ensure that it provides a sound basis for the evaluation. The sponsor should be notified of any problems so that the security target can be amended prior to the start of the evaluation.



4.2 Technical Oversight

Technical oversight is the general process employed by the CCEVS to ensure that the evaluation and validation activities taking place within the scheme are being conducted in accordance with the provisions of the Common Criteria, the Common Methodology, and the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security*, and any scheme-specific policies and procedures. Technical oversight involves the monitoring of CCTLs and the monitoring of specific evaluations.

CCEVS shall assign a technical representative, or validator, to each IT security evaluation to serve as the primary point of contact for the CCTL and sponsor of the evaluation. The CCTL and sponsor shall also assign a point of contact to interact with the CCEVS during the evaluation. The CCEVS shall have its technical representative monitor the evaluation and perform a variety of validation activities as described in [Publication #3, *Guidance to Validators*](#)..

4.2.1 CCTL Accreditation and Monitoring

The Common Criteria Scheme focuses on the laboratory accreditation process to ensure that commercial testing facilities have the requisite capability to conduct quality security evaluations of IT products and protection profiles in a consistent manner. However, the complexity of IT security evaluations with the dual requirements for design analysis and testing makes these types of evaluations unique. This complexity and need for consistency across the scheme to ensure fairness for all participating CCTLs, make technical oversight essential.

Technical oversight involves monitoring the CCTLs. The CCEVS staff ensures consistency amongst CCTLs through frequent contact with CCTL personnel, CCTL meetings, labgrams, etc.

CCEVS validators monitor CCTLs during each evaluation in two ways: by ensuring that the CCTL is following their documented quality processes (i.e., conflict of interest policies, record-keeping processes, evaluator training processes, etc.); and by performing Validation Oversight Reviews (VORs) at various points during the evaluation to ensure the technical soundness of the work performed by the evaluation team (i.e., correct application of the CC, technical accuracy of the evaluation analysis, thorough testing during the evaluation, etc.).

4.2.2 Scope of Technical Oversight

Oversight will be exercised by the CCEVS as required to adequately ensure that the CCTL has correctly and completely applied the Common Criteria and the Common Methodology for the specific IT security evaluation and level of assurance sought. The purpose of evaluation monitoring is to mitigate risk among all participants in the scheme,

(i.e., the CCEVS, CCTLs, and sponsors of evaluations). In general, the number, type, and intensity of activities associated with the oversight process will be a function of:

- a) the assurance requirements, (i.e., predefined Common Criteria evaluation assurance level or sponsor-defined assurance package), that appear in the security target;
- b) the complexity of the Target of Evaluation (TOE); and
- c) the experience of the CCTL in evaluating IT products in the identified technology area.

The CCEVS has strict guidelines on how these technical oversight activities will be implemented within the scheme in order to establish the appropriate level of expectation on behalf of sponsors and CCTLs. The specific details of the technical oversight process and activities associated with that process are described in [Publication #3](#), *Guidance to Validators*.

4.3 Conduct of the IT Security Evaluation and Validation

Evaluation is the assessment of an IT product for conformance to the Common Criteria. The evaluation determines how well the product, or TOE, meets the functional and assurance security requirements contained in its security target. The objective is to enable the CCTL conducting the evaluation to prepare an impartial report stating whether or not the TOE satisfies its security target.⁷

Validation oversight provides independent confirmation that an IT security evaluation has been conducted in accordance with the provisions of the scheme and that the conclusions of the CCTL are consistent with the facts presented in their evaluation technical report.

4.3.1 Entering the Scheme

Once the CCTL has obtained the necessary documentation and completed any required analysis, they should prepare for an Initial Validation Oversight Review (IVOR) with CCEVS. The CCTL shall submit an IVOR read-ahead package (as outlined in the Validation Oversight Review (VOR) Evaluator's and Validator's Guide). Upon completion of a successful IVOR, a Kick-off meeting between the sponsor/vendor, the CCTL and the CCEVS will be scheduled. Upon successful completion of the kick-off meeting, the product is considered to be in evaluation and will be posted on the CCEVS web site on the "Products in Evaluation" list.

⁷The first phase of a formal security evaluation is the evaluation of the security target itself in accordance with the requirements described in the Common Criteria and Common Methodology. Following security target evaluation, the IT product, or TOE, is evaluated against the security target. These activities are occasionally interleaved during an evaluation

4.3.2 Evaluation Activities

The CCTL conducts the IT security evaluation of the TOE according to the evaluation work plan using the deliverables specified in the deliverables list. The work plan may evolve during the evaluation as additional information is made available to the CCTL by the sponsor. The CCTL is encouraged to consult with the CCEVS at any time to discuss technical matters, anomalies which may arise, or any other issues relevant to the evaluation.

The results of the IT security evaluation are documented by the CCTL as the evaluation proceeds. The sponsor and CCTL shall inform the CCEVS through *observation reports*⁸ of issues that arise during evaluation to include problems found in the TOE and any problems related to the Common Criteria or Common Methodology. In general, CCTLs should be interacting directly with sponsors to resolve issues and address problems that arise during an evaluation. Observation reports should be submitted only in situations where specific issues or problems could not be resolved by the sponsor and CCTL or guidance or interpretation from the CCEVS is required.

In situations where the issue or problem is related to the Common Criteria, the Common Methodology, or the scheme, the CCEVS will take the following actions, in turn, upon receipt of the observation report:

- a) assess the immediate issue or problem and render an initial decision for that particular IT security evaluation;⁹
- b) address the issue or problem within scheme channels, employing the services of technical working groups with security and testing community representation from CCTLs and other technical experts as needed;
- c) if necessary, address the problem or issue formally within international channels in accordance with established procedures and involving relevant standards groups, technical committees, or other appropriate bodies.

In situations where the issue or problem is product-related, the sponsor shall provide the CCEVS and the CCTL a detailed proposal for the resolution of the issue or problem noted in the report and the timeframe for such activity. If it is not possible to resolve a particular issue or problem, and the CCEVS decides that the evaluation will be affected, the CCEVS shall contact the sponsor to discuss the potential impact and possible alternatives. Based on the contract with the CCTL, the sponsor may abandon the IT security evaluation, consult with the CCEVS to discuss continuing the security evaluation

⁸An observation report is a vehicle by which a CCTL or sponsor of an evaluation requests a clarification of scheme related information or identifies an anomaly in the evaluation. Observation reports can also be submitted by members of the CCEVS. Typically, the report will contain the observation, severity of the observation, organization responsible for resolving the issue, timetable for resolution of the issue, and impact on the evaluation if the issue is not resolved.

⁹The purpose of this immediate decision is to expedite the IT security evaluation and not adversely impact the CCTL's evaluation schedule. The decision applies only to the current evaluation in question (on a temporary, one-time basis) and is to be subsequently considered in a more formal setting by the appropriate technical committees or working groups either within the scheme or through counterpart organizations within the international community.

while accepting the problem and its implication for validation or reschedule the security evaluation and, in consultation with the CCEVS, ensure that the TOE is modified, as needed.

4.3.3 The Validation Oversight Review (VOR) Process

The primary goal of the Validation Oversight Review (VOR) process is for CCEVS to ensure the technical quality and consistency of the evaluation, to confirm that the CCTL correctly applied all CCEVS policies, and to verify the CCTL accomplished all required tasks (including analysis, testing, auditing, etc).

The number of VORs for a specific evaluation shall be determined at the beginning of the evaluation. Following is a brief description of each type of VOR:

The Initial VOR shall ensure that the ST is accurate and clearly specified, meets all relevant CCEVS policies and their respective addendums, and that the evaluation team correctly performed the Assurance Security Target Evaluation (ASE) analysis.

The Test VOR shall be scheduled after the ST passes all the required work units (except those dependent on testing activities) and the evaluators have thoroughly reviewed the developer test plan and created the evaluation team test plan. The Test VOR shall review those activities performed in ADV and ATE. Since the proper identification of the TSF and TSFI are critical to the testing effort, the Test VOR shall address these areas along with the test planning.

The Final VOR shall focus on reviewing and discussing the evaluation team's testing and ensuring all previously identified issues have been resolved.

All VORs shall conclude with a draft VOR Report containing a list of agreed upon issues and actions.

Additional details on the VOR process can be found in the [Validation Oversight Review \(VOR\) Evaluator's and Validator's Guide](#).

4.4 Conclusion of the Evaluation

The findings of the IT security evaluation are documented by the CCTL in an evaluation technical report. The content and presentation of evidence in the report shall be in accordance with the Common Criteria and Common Methodology. The CCTL shall ensure that the evaluation technical report is structured in such a way as to allow for the removal of proprietary or sensitive information.

The sponsor may contact the CCTL concerning any statements in the report which the sponsor believes to be misleading, unjustified, or inaccurate.

Upon completion of the security evaluation, the CCEVS validator reviews the evaluation technical report produced by the CCTL, discusses it with the evaluators during the final Validation Oversight Review (FVOR) and determines the extent to which the security

target is met by the TOE. In the case of a protection profile evaluation, the review determines the extent to which the profile is shown to be complete, consistent, and technically sound. The CCEVS validator also confirms that the evaluation was conducted in accordance with the Common Criteria, Common Methodology, and procedures required by the scheme and that the report provides a suitable basis for the final validation report.

The CCEVS validator reserves the right to contact the CCTL to obtain additional information for clarification of evaluation-related issues and/or to obtain access to specific evidence and results to support any conclusions presented in the evaluation technical report. The specific activities involved in the review process are described in [Publication #3, *Guidance to Validators*](#).

4.5 Evaluation of Protection Profiles

The goal of protection profile evaluation is to demonstrate that the profile is complete, consistent, and technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated. The sponsor is responsible for providing the protection profile to the CCTL conducting the evaluation. In addition, the sponsor may want to provide the CCTL any relevant documentation associated with the development of the protection profile.

The CCEVS requires both the protection profile and the evaluation schedule from the sponsor and the CCTL before accepting the prospective protection profile evaluation into the scheme.

As with IT product evaluations, the findings of the protection profile evaluation are documented by the CCTL in an evaluation technical report. The content and presentation of evidence in the report shall be in accordance with the appropriate sections of the Common Criteria and the Common Methodology. The report is submitted to the CCEVS and to the sponsor of the evaluation. The sponsor may contact the CCTL concerning any statement in the protection profile evaluation technical report which the sponsor believes to be misleading, unjustified, or inaccurate.

5 Common Criteria Certificates

Once the final validation report has been approved by the CCEVS, a Common Criteria certificate will be issued. NSA is the certificate-issuing authority for the CCEVS. The Director of the CCEVS and a senior executive from the agency will sign the certificate, indicating acceptance of the points articulated above. After the certificate has been issued for the security evaluation, an appropriate entry will be made on the CCEVS Validated Products List.

5.1 Proper Use of CC Certificate

The certificate applies only to the specific version and release of the IT product in its evaluated configuration or the particular version of the protection profile as evaluated. A sponsor of an evaluation shall only market an IT product or a protection profile as an evaluated product or an evaluated profile, respectively, on the basis of the validation report and accompanying Common Criteria certificate published by the CCEVS. The issuance of a certificate does not imply endorsement of an IT product or protection profile by NSA, or any other agency of the U.S. Government. Additional details on Common Criteria certificates can be found in [Publication #2 Quality Manual and Standard Operating Procedures](#) and [Annex D](#).

5.2 Certificate Maintenance

Procedures for the maintenance of Common Criteria certificates, (e.g., in conjunction with extensions to later releases or versions of the IT product or protection profile), are governed by the Common Criteria Certificate Maintenance Program as described in [Publication #6 Assurance Continuity: Guidance for Maintenance and Re-evaluation](#). A sponsor, anticipating the need for re-evaluation, may wish to consider a certificate maintenance approach at early stages of the initial evaluation in order to minimize future evaluation activities. Sponsor coordination with a CCTL may be required in order to take re-evaluation or certificate maintenance requirements into account when performing the initial evaluation of the IT product or protection profile. Specific details of the certificate maintenance process employed within the scheme are provided in [Publication #6 Assurance Continuity: Guidance for Maintenance and Re-evaluation](#).

Annex A: References

The Report of the [President's Commission on Critical Infrastructure Protection](#) (PCCIP), *Critical Foundations: Protecting America's Infrastructures*, October, 1997.

The White House, The Clinton Administration's Policy on Critical Infrastructure Protection: [Presidential Decision Directive 63, May 1998](#).

CEMEB (Common Evaluation Methodology Editorial Board), [Common Methodology](#) for Information Technology Security Evaluation, Version 3.1, September 2007.

CCMB (Common Criteria Maintenance Board), [Common Criteria](#) for Information Technology Security Evaluation, Version 3.1, September 2007.

Part 1 Introduction and general model

Part 2 Security functional components

Part 3 Security assurance components

[NIST Handbook 150:2005](#) Edition, *Procedures and General Requirements*

[NIST Handbook 150-20](#), *Information Technology Security Testing—Common Criteria*

[ISO/IEC 17025](#) (formerly ISO Guide 25)—General Requirements for the Competence of Calibration and Testing Laboratories, 2005

[ISO/IEC Guide 65](#) — General Requirements for Bodies Operating Product Certification Systems, 1996

Annex B: Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCMB	Common Criteria Maintenance Board
CEM	Common Evaluation Methodology
CCRA	Common Criteria Recognition Arrangement
CCTL	Common Criteria Testing Laboratory
EAL	Evaluation Assurance Level
EAP	Evaluation Acceptance Package
ETR	Evaluation Technical Report
FVOR	Final Validation Oversight Review
ISO	International Organization for Standardization
IVOR	Initial Validation Oversight Review
NIAP	National Information Assurance Partnership
MR	Memorandum for Record
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
OD	Observation Decision
OR	Observation Report
ODRB	Observation Decision Review Board
PP	Protection Profile
ST	Security Target

TOE	Target of Evaluation
TTAP	Trust Technology Assessment Program
TOP	Technical Oversight Panel
TVOR	Test Validation Oversight Review
VID	Validation Identification
VOR	Validation Oversight Review
VPL	Validated Products List
VR	Validation Report

Annex C: Glossary

This glossary contains definitions of terms used in the Common Criteria Scheme. These definitions are consistent with the definitions of terms in ISO Guide 2 and are also broadly consistent with the Common Criteria and Common Methodology.

Accreditation Body: An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard.

Agreement Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security: An agreement in which the Parties (i.e., signatories from participating nations) agree to commit themselves, with respect to IT products and protection profiles, to recognize the Common Criteria certificates which have been issued by any one of them in accordance with the terms of the agreement.

Appeal: The process of taking a complaint to a higher level for resolution.

Approved Test Methods List: The list of approved test methods maintained by the CCEVS which can be selected by a CCTL in choosing its scope of accreditation, that is, the types of IT security evaluations that it will be authorized to conduct using CCEVS-approved test methods.

Assurance Maintenance: The process of recognizing that a set of one or more changes made to a validated TOE has not adversely affected assurance in that TOE.

Assurance maintenance addendum: A notation, such as on the listing of evaluated products, that serves as an addendum added to the certificate for a validated TOE. The maintenance addendum lists the maintained versions of the TOE.

Impact Analysis Report (IAR): A report which records the analysis of the impact of changes to the validated TOE.

Assurance Continuity Maintenance Process: A program within the Common Criteria Scheme that allows a sponsor to maintain a Common Criteria certificate by providing a means (through specific assurance maintenance requirements) to ensure that a validated TOE will continue to meet its security target as changes are made to the IT product or its environment.

Assurance Maintenance Report: A publicly available report that describes all changes made to the validated TOE which have been accepted under the maintenance process.

Common Criteria (CC): Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

Common Criteria Certificate: A certificate issued by the CCEVS which confirms that an IT product or protection profile has successfully completed evaluation by an accredited CCTL in conformance with the Common Criteria standard.

Common Criteria Evaluation and Validation Scheme (CCEVS): The program developed to establish an organizational and technical framework to evaluate the trustworthiness of IT products and protection profiles.

Common Criteria Testing Laboratory (CCTL): Within the context of the Common Criteria Evaluation and Validation Scheme, an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS to conduct Common Criteria-based evaluations.

Common Evaluation Methodology (CEM): Common Methodology for Information Technology Security Evaluation, the title of a technical document which describes a particular set of IT security evaluation methods.

Evaluation Evidence: Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

Evaluation Technical Report: A report giving the details of the findings of an evaluation, submitted by the CCTL to the CCEVS as the principal basis for the validation report.

Evaluation Work Plan: A document produced by a CCTL detailing the organization, schedule, and planned activities for an IT security evaluation.

Interpretation: Expert technical judgment, when required, regarding the meaning or method of application of any technical aspect of the Common Criteria and/or Common Methodology.

National Voluntary Laboratory Accreditation Program (NVLAP): The U.S. accreditation authority for CCTLs operating within the NIAP Common Criteria Evaluation and Validation Scheme.

National Information Assurance Partnership (NIAP): The partnership that included the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) which established a program to evaluate IT product conformance to international standards. Currently, NIST is responsible for the National Voluntary Laboratory Accreditation Program (NVLAP) and NSA is responsible for the Common Criteria Evaluation and Validation Scheme (CCEVS).

Observation Decision (OD): The formal documented response from the CCEVS that provides clarification/guidance to the CCTL on a submitted Observation Report.

Observation Reports (OR): A report issued to the CCEVS by a CCTL or sponsor identifying specific problems or issues related to the conduct of an IT security evaluation.

Protection Profile (PP): An implementation independent set of security requirements for a category of IT products which meet specific consumer needs.

Re-evaluation: A process of recognizing that changes made to a validated TOE require independent evaluator activities to be performed in order to establish a new assurance baseline. Re-evaluation seeks to reuse results from a previous evaluation.

Security Target (ST): A specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation under the Common Criteria. The security target specifies the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

Target of Evaluation (TOE): A TOE is defined as a set of software, firmware and/or hardware possibly accompanied by guidance.

Technical Oversight Panel: A panel composed of scheme validators to ensure technical consistency across evaluations and validations performed under CCEVS.

Validation: The process carried out by the CCEVS leading to the issue of a Common Criteria certificate.

Validation Oversight Review: The process for CCEVS to provide validation oversight and to ensure the technical quality of evaluations.

Initial VOR: To ensure that the ST is accurate and clearly specified, meets CCEVS Policies 1, 9, 10, 13, their respective addendums, and the evaluation team correctly performed the Assurance Security Target Evaluation (ASE) analysis

Test VOR: The Test VOR shall be conducted after the TOE passes all the work units except those dependent on team testing. Examples of these exceptions include some (not all) of the guidance documents, testing and vulnerability analysis work units.

Final VOR: The focus of the Final VOR is to ensure all issues have been resolved and to discuss the evaluation team's testing activities.

Validated Products List (VPL): A publicly available listing maintained by the CCEVS Scheme of every IT product/system or protection profile that has been issued a Common Criteria certificate by the CCEVS.

Validation Report (VR): A document issued by the CCEVS and posted on the VPL which summarizes the results of an evaluation and confirms the overall results.

Annex D: Common Criteria Certificates

The following information shall be included on all Common Criteria certificates issued by the CCEVS. In addition to the information listed, the mutual recognition mark shall be placed on each Common Criteria certificate issued by the CCEVS. The certificate is only valid in conjunction with the full validation report produced for its associated IT product or protection profile evaluation.

D-1 Certificates Associated with IT Product Evaluations

A Common Criteria certificate issued by the CCEVS resulting from the validation of an IT product evaluation shall include the following information:

- a) Product developer;
- b) Product name;
- c) Version and release numbers;
- d) Protection profile identifier (if claiming conformance);
- e) Evaluation platform;
- f) Name of CCTL;
- g) Validation report number;
- h) Date issued;
- i) Assurance level;
- f) Signature of Director, Common Criteria Evaluation and Validation Scheme;
- j) Signature of Information Assurance Director, National Security Agency;
- k) A statement indicating that:
 - 1) The IT product has been evaluated at an accredited testing laboratory using the Common Methodology for Information Technology Security Evaluation (version number) for conformance to the Common Criteria for Information Technology Security Evaluation (version number) as articulated in the product's functional and assurance security specification contained in its security target;
 - 2) The evaluation has been conducted in accordance with the provisions of the Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence presented;

3) The issuance of a certificate is not an endorsement of the IT product by NSA, or any agency of the U.S. Government and no warranty of the product is either expressed or implied;

4) The certificate applies only to the specific version of the product in its evaluated configuration.

A sample product-related Common Criteria certificate is provided in Figure D-1.

	National Information Assurance Partnership Common Criteria Certificate	
<i>is awarded to</i> Company Name		
<p>The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version X) for conformance to the Common Criteria for IT Security Evaluation (Version X). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.</p>		
Product Name: Version: Evaluation Platforms:		CCTL: Validation Report Number: Date Issued: Protection Profile Identifier: Assurance Level:
<hr/> <i>Director, Common Criteria Evaluation and Validation Scheme</i> National Information Assurance Partnership		<hr/> <i>Information Assurance Director</i> National Security Agency

Figure D-1. Sample Common Criteria Certificate for an IT Product

D-2 Certificates Associated with Protection Profile Evaluations

A Common Criteria certificate issued by the CCEVS resulting from the validation of a protection profile evaluation shall include the following information:

- a) Protection profile name/identifier;
- b) Version number;
- c) Name of CCTL;
- d) Validation report number;
- e) Date issued;

- f) Signature of Director, Common Criteria Evaluation and Validation Scheme;
- f) Signature of Information Assurance Director, National Security Agency;
- g) A statement indicating that:
 - 1) The protection profile has been evaluated at an accredited testing laboratory using the Common Methodology for Information Technology Security Evaluation (version number) for conformance to the Common Criteria for Information Technology Security Evaluation (version number);
 - 2) The evaluation has been conducted in accordance with the provisions of the Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence presented;
 - 3) The issuance of a certificate is not an endorsement of the protection profile by NSA, or any agency of the U.S. Government and no warranty of the profile is either expressed or implied;
 - 4) The certificate applies only to the specific version of the protection profile as evaluated. A sample profile-related Common Criteria certificate is provided in Figure E-2.

A sample profile-related Common Criteria certificate is provided in Figure D-2.



National Information Assurance Partnership
Common Criteria Certificate



National Security Agency

The protection profile identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version X) for conformance to the Common Criteria for IT Security Evaluation (Version X). This certificate applies only to the specific version of the protection profile as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the protection profile by any agency of the U.S. Government and no warranty of the protection profile is either expressed or implied.

Protection Profile Name/Identifier:
Version Number:

Name of CCTL:
Validation Report Number:
Assurance Package:

Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Information Assurance Director
National Security Agency

Figure D-2. Sample Common Criteria Certificate for a Protection Profile