National Information Assurance Partnership
Common Criteria/
Evaluation and Validation Scheme

Publication #5

Guidance to Sponsors

April 2014
Version 3.0

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

National Security Agency
Common Criteria Evaluation and Validation Scheme
9800 Savage Road, Suite 6940
Fort George G. Meade, MD 20755-6940
E-mail: niap@niap-ccevs.org
http://www.niap-ccevs.org/cc-scheme

Amendment record

Version	Date	Description
Draft 1.0	31 August 2000	Initial release.
2.0	8 September 2008	Complete revision based on current operations
3.0	April 2014	Updates

(Page intentionally left blank)

Table of Contents

1 Introduction 1

1.1 Purpose of this document 1
1.2 Organization and Scope 2

2 Common Criteria Evaluation Overview 3

2.1 Protection Profile (PP) 3
2.2 Target of Evaluation (TOE) 3
2.3 Security Target (ST) 4

3 NIAP Assistance and Services 5

3.1 Answers to Scheme Questions 5
3.2 Requests for CC and PP Interpretation 5
3.3 Validation Services 5

4 Sponsor Guidance 6

4.1 Phase I 6
4.1.1 Selecting a CCTL 6
4.1.2 Consulting Support 6
4.1.3 Preparation for Evaluation 7
4.1.4 Evaluation Goals 7
4.1.5 Deliverables 7
4.1.6 Readiness for Evaluation 9
4.1.7 Entering the Scheme (NIAP) 9
4.1.8 Proprietary/Sensitive Information 9
4.1.9 Sponsor Responsibilities 10
4.1.10 Sponsor's Expectations of the CCTL 10
4.1.11 Sponsor's Expectations of NIAP 10
4.2 Phase II 11
4.2.1 Sponsor's Responsibilities 11
4.2.2 Sponsor's Expectations of CCTL during Phase II 11
4.2.3 Sponsor's Expectations of Validator during Phase II 11
4.2.4 Complaints and Appeals 12
4.3 Phase III 12
4.3.1 Certificate Issuance 12
4.3.2 Evaluation Records Management 13
4.3.3 Sponsor Responsibilities Pertaining to Phase III 13
4.4 Phase IV 13
4.4.1 Common Criteria Certificate Maintenance 13
4.4.2 Certificate use monitoring 13
4.4.3 Sponsor responsibilities during Phase IV 14

Annex A: References 15

Annex B: Acronyms 16

Annex C: Glossary 17
Annex D: Common Criteria Certification Mark Policy 20

1 Introduction

The Common Criteria Evaluation and Validation Scheme (CCEVS) for Information Technology Security was established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to validate conformance of Information Technology (IT) products to international standards. The CCEVS oversees the evaluations performed by Common Criteria Testing Labs (CCTLs) on information technology products against the *Common Criteria for Information Technology Security Evaluation* (CC).

The principal participants in the CCEVS program are the:

- **Sponsor**: The Sponsor may be a product developer, a value-added reseller of an IT security-enabled product, or another party that wishes to have a product evaluated. The sponsor requests that a Common Criteria Testing Laboratory (CCTL) conduct a security evaluation of an IT product.

- **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.

1.1 Purpose of this document

The purpose of this document is to provide guidance and assistance to the sponsor of an IT product evaluation under the CCEVS. It will help the sponsor prepare for and understand their responsibilities prior to, during, and after an evaluation. Additionally, what the sponsor can expect of the CCTL and the CCEVS is identified.

The *sponsor* is the individual or organization requesting a security evaluation of an IT product. The relationship of the sponsor to the IT product may vary depending on the nature of the product and the circumstances surrounding the evaluation. In most cases, the sponsor of a security evaluation will be the actual developer of the IT product. 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 the product.

When the sponsor of an evaluation is not the developer of the product, the sponsor must work cooperatively with the developer. Regardless of whether or not the sponsor is the developer, the CCTL must be provided with the technical materials and essential

deliverables needed to conduct the IT security evaluation in a complete and consistent manner. The details of the provision of materials for the security evaluation will be handled in contractual agreements between the sponsor and the developer.

1.2 Organization and Scope

This document is one of a series of technical and administrative CCEVS publications that describes how the scheme operates. It consists of four chapters and several supporting annexes. Chapter 1 provides a high level overview of the validation process. Chapter 2 provides an overview of the Common Criteria Evaluation. Chapter 3 provides information related to CCEVS Assistance and Services, and Chapter 4 provided Sponsor Guidance.

The supporting annexes cover a variety of topics to include an acronym list, a glossary, a list of references and the Common Criteria Certification Mark.

This document complements or references other CCEVS publications and documents used in the operation of the CCEVS. These other publications include:

Publication #1: *Organization, Management, and Concept of Operations*

Publication #2: *Quality Manual and Standard Operating Procedures*

Publication #3: *Guidance to Validators*

Publication #4: *Guidance to CCEVS-Approved Common Criteria Testing Laboratories*

Publication #5: *Guidance to Sponsors*

Publication #6: *Assurance Continuity: Guidance for Maintenance and Re-evaluation*

CCEVS related publications and information are available through the CCEVS web site at http://www.niap-ccevs.org/cc-scheme/index.cfm.

2 Common Criteria Evaluation Overview

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 Common Criteria Scheme provides consumers with an impartial assessment of an IT product by an independent entity. This impartial assessment includes an analysis of the IT product and the testing of the product for conformance to a set of security requirements. IT security evaluations are composed of analysis and testing, distinguishing these activities from the more traditional forms of conformance testing in other areas.

The application of the CC is expressed through the following documents:

- Protection Profile (PP)
- Target of Evaluation (TOE)
- Security Target (ST)
- Common Evaluation Methodology (CEM)

2.1 Protection Profile (PP)

The CC defines a PP as an implementation independent set of security requirements for a category of IT products, which meet specific consumer needs. The PP is essentially a system design document starting with a statement of need and refines it though several levels to a solution that meets the need. It is not just a set of requirements but a framework for defining requirements that shows what is addressed and gives the context for relating the requirement set to a specific user's needs.

A PP:

- identifies the security capability to be provided,
- specifies conformances claims of a security target claiming compliance to the PP,
- describes the IT portion of the solution that is the subject of this requirement set,
- describes the environment in which the security issues are to be addressed,
- gives the security objectives that, when met, will provide the identified security capability,
- specifies the security requirements (function and assurance) needed to accomplish this, and
- provides a rationale showing the specified requirements do in fact provide the identified security capability.

2.2 Target of Evaluation (TOE)

The target of evaluation (TOE) is a set of software, firmware and/or hardware and its associated documentation that is the subject of a security evaluation under the Common Criteria.

The TOE is the IT product that is the subject of the requirement set being specified by the PP (or the ST described below). Additionally, the TOE is the security-related user and administrator guidance associated with the IT product.

2.3 Security Target (ST)

While the PP is implementation independent, an ST is 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 ST, like a PP, specifies:

- the security capability to be provided,
- the PP to which the product claims exact conformance,
- the environment in which this capability is to be provided,
- the security objectives that, when met, will provide the needed capability in the specified environment, and
- the specific security requirements (functional and assurance) needed to accomplish this.

In addition, the ST identifies the specific security mechanisms that will be employed, and indicates the PP(s), if any, with which the ST is compliant.

The ST is derived from a PP. The ST is used to describe the security characteristics of existing IT product and provides a common format for describing security requirements. The ST, unlike previous requirement sets and most existing vendor produced product descriptions, gives context for the requirements and provides a rationale for why the requirements implement the claimed capabilities.

In order for evaluations conducted in different testing laboratories to meet a common set of expectations, a standard evaluation methodology is needed. This is provided by the CEM. The CEM provides, for each assurance component, a specified set of work units to be performed. Along with each work-unit is text describing the nature of the work to be performed.

3 NIAP Assistance and Services

NIAP provides both assistance and services to customers. Assistance provided by NIAP includes: responding to customer inquiries; holding/attending informational meetings; conducting workshops; providing educational resources; providing the latest information on Scheme processes and procedures; and providing guidance on the type of evidence required for an evaluation. NIAP does not provide services for preparing sponsor material for the evaluation or in the collection or preparation of evidence. NIAP assistance is provided without charge.

3.1 Answers to Scheme Questions

Prior to the start of an evaluation, potential sponsors may have questions about the Scheme. The sponsor should review the NIAP Guidance Publications or Frequently Asked Questions (FAQ) to see if these sources provide the answers needed.

3.2 Requests for CC and PP Interpretation

A common request is for interpretation of the CC or the PP. NIAP will respond to general questions by telephone or email to a rapid response team. However, the required method for submitting specific questions about criteria interpretation is in writing (by letter or email). NIAP will provide a written response to all requests for interpretation.

Before submitting a request for criteria interpretation, the sponsor should:

a) Review the Common Criteria Maintenance Board's (CCMB) current list of interpretations to see if the current available interpretations provide the necessary answers.
b) Review any NIAP technical decisions not covered by the CCMB interpretations to determine if these provide the necessary information. For more information, please see the following page: https://www.niap-ccevs.org/Documents_and_Guidance/view_tds.cfm

3.3 Validation Services

The primary focus of NIAP is to provide validation oversight to CCTL evaluations. Validation services are the activities followed in assuring a given IT product evaluation has been conducted in accordance with the provisions of NIAP, CC, and CCRA; ensuring the results of the IT security evaluations produced by the CCTLs are validated; and when all the required NIAP conditions have been met, issuing a Common Criteria Certificate for the IT product. The specific validation activities to be performed by NIAP for an IT product evaluation are defined in the Check-In Check-Out (CICO) Guidance.

NIAP currently provides validation services for sponsors and CCTLs at no charge. The actual cost of these services, to include technical oversight and monitoring, final issuance of Common Criteria certificate, publication of Validation Reports (VR), and the posting of IT products and PPs on the NIAP Product Compliant List (PCL) will be monitored and assessed. NIAP may initiate a cost-recovery program for validation services in the future.

4 Sponsor Guidance

This section provides guidance relevant to sponsors during the course of an evaluation. NIAP utilizes a Check In/Check Out (CICO) process to validate CCTL evaluations. CCTL milestones associated with the CICO process include Check-in, Sync Sessions, and Check-Out. For the details on how CCTL evaluations are validated, see Publication #3 and the CICO Guide.

Phase I includes any activity occurring prior to the Kick-off meeting.

Phase II begins at the Check-In meeting and concludes once the Check in receives a passing verdict.

Phase III begins once the Check in receives a passing verdict and the CCTL delivers all evaluation documentation to the validator and ends with CC certificate issuance and PCL posting.

Phase IV includes all follow-on activity such as Assurance Continuity and certificate monitoring.

4.1 Phase I

The primary sponsor responsibility during phase I is to prepare for the CC evaluation and validation process. Information may be gathered from a variety of sources, including consulting with a CCTL or other company, open source literature, and contacting NIAP. The sponsor is also responsible for providing the required material for the CC evaluation, and securing the appropriate legal and nondisclosure agreements with the CCTL.

4.1.1 Selecting a CCTL

The list of accredited CCTLs is located at the NIAP web site. When selecting a CCTL for consulting prior to an evaluation, or for performing the evaluation, or both, the sponsor should use a careful screening process. The experience of the CCTL personnel with the technology and PP comprehension, the fees, the estimated schedule, and any other pertinent factors should be reviewed and considered before the sponsor enters into a contractual relationship with a CCTL. Details of the contract between the CCTL and the sponsor are left to the two parties to negotiate, with no involvement by NIAP.

4.1.2 Consulting Support

It is important to note there must be no apparent or perceived conflict of interest between those individuals performing consulting services for an evaluation and the evaluation team personnel. Specifically, there must be a clear and definite separation of personnel between these two functions. If a CCTL is used for both consulting and evaluation, contract negotiations between the CCTL and the sponsor should clearly specify that different personnel must be used for the two different functions.

The scope of consulting work during the preparation for an IT security evaluation is not controlled by the Scheme and is a matter of negotiation between the sponsor and the

CCTL or other consultant. However, the CCTL must adhere to the terms and conditions of its NVLAP accreditation to ensure the advice given does not affect evaluator independence or impartiality in any evaluation.

4.1.3 Preparation for Evaluation

The majority of activity in the early stages of an evaluation occurs between the sponsor of the evaluation and the CCTL. The sponsor is responsible for providing the ST and the associated Target of Evaluation (TOE). The composition of a TOE may vary and may 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. The sponsor must ensure that arrangements have been made to provide all essential documentation to the CCTL evaluation team in order to conduct a successful security evaluation.

4.1.4 Evaluation Goals

4.1.4.1 PP Evaluation

Evaluating a PP is required to demonstrate the PP is sound and internally consistent. PP evaluations may be standalone (i.e., the PP is evaluated against the APE class of the CC) or may be conducted as part of the first product evaluation against the PP. NIAP does not conduct standalone PP evaluations, but rather performs evaluation of all PPs as part of the first product evaluation against the PP. Upon successful completion of a product evaluation against the PP, the PP is considered evaluated for the purposes of Mutual Recognition under the CCRA and is listed on the CC portal website.

In addition to the PP, the sponsor may want to provide the CCTL with any relevant documentation associated with the development of the PP.

4.1.4.2 TOE Evaluation

The goal of a TOE evaluation is two-fold:

a) to demonstrate that the ST is complete, consistent, and technically sound, meets any PP compliance claims and, hence is suitable for use as a statement of requirements for the TOE; and demonstrate that the TOE complies exactly with the requirements specified in the PP.

4.1.5 Deliverables

A TOE evaluation requires the development and delivery of a ST.

The ST serves as both a specification of the security functions against which the TOE will be evaluated and as a description relating the product to the environment in which it will operate. The ST includes a list of claims about the TOE made by the sponsor, which must be exact conformance to a PP.

The deliverables for the evaluation of a TOE against its ST are typically items of hardware, firmware, software, and technical documentation normally generated during the development of the product. Additional TOE security-relevant documentation must be developed and delivered as required by the assurance requirements in the ST.

Appropriate contractual arrangements shall be made by the sponsor to ensure evaluation deliverables are provided 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 contractual arrangements include authority for the release of previous evaluation results if reuse of these results is desired.

4.1.5.1 Sources and Guidance for Producing STs and PPs

The content and presentation of both a PP and an ST must be specified in terms of the Common Criteria.

The development of a PP or ST can be a challenging task for those who are not experienced in writing such documents. Several sources exist to aid in developing PPs and STs. These sources are listed below.

a) **Existing PPs and STs:** Final PPs are available on the NIAP web site. A list of Compliant Products and associated NIAP VRs and STs are posted on the PCL.
b) **Commercial Companies:** Many of the CCTLs offer consulting services for helping vendors or sponsors develop STs. Security engineering firms or consultants well versed in the Common Criteria are also potential sources of assistance. As noted earlier, there can be no appearance of bias or conflict of interest by those conducting evaluations. Therefore, the sponsor must ensure the ST consultants will have no involvement in the product evaluation. The list of accredited CCTLs can be found at the following web site: http://www.niap-ccevs.org/Big_Picture/cctls.cfm
c) **ISO 15408 Common Criteria Standard**: The Common Criteria for Information Technology Security Evaluation (CC), ISO 15408, defines the structure, presentation, and content of both a PP and a ST. The CC also serves as a catalog of CC IT security functional and assurance requirements. The CC can be found on the web at: http://www.commoncriteriaportal.org/thecc.html or http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
d) **Guide for the Production of PPs and STs:** ISO/IEC TR 15446:2004 provides guidance relating to the construction of PPs and STs intended to be compliant with ISO/IEC 15408 (the "Common Criteria"). ISO/IEC TR 15446:2004 gives suggestions on how to develop each section of a PP or ST. It is supported by an annex containing generic examples of each type of PP and ST component, and by other annexes that contain detailed worked examples. ISO/IEC TR 15446:2004 is primarily aimed at those who are involved in the development of PPs and STs. However, it is also useful to evaluators and those who are responsible for monitoring PP and ST evaluations. It may also be of interest to consumers and users of PPs and STs who wish to understand what guidance the PP/ST author

used, and which parts of the PP or ST are of principal interest. For more information, see http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39690

4.1.6 Readiness for Evaluation

Once the sponsor has established the ST and the strategy for the supply of deliverables, the sponsor should select a CCTL to conduct the evaluation of the IT product. A sponsor may provide potential CCTLs with the completed ST in order to obtain more accurate evaluation proposals. The CCTL selected to conduct the evaluation should review the ST to ensure it provides a sound basis for the evaluation. The sponsor should address any issues raised in the ST prior to the start of the evaluation. When a successful evaluation seems feasible, the CCTL should prepare an *Evaluation Schedule*, and perform the Assurance ST Evaluation (ASE) analysis. Upon successful completion of the ASE analysis, the CCTL prepares to enter the evaluation into the Scheme.

4.1.7 Entering the Scheme (NIAP)

The CCTL will provide NIAP with an Initial Check In package. The CICO process is used by NIAP to accept and oversee the product during its evaluation. The CICO process requires the successful completion of an Initial Check In prior to evaluation acceptance. For details of the CICO process, see the Check In/Check Out Evaluators and Validators Guide.

4.1.8 Proprietary/Sensitive Information

4.1.8.1 Access to Proprietary/Sensitive Information

The sponsor must ensure the CCTL and NIAP are provided with all the IT product related information and materials needed in order to complete the evaluation and validation process. Some of the required information may be proprietary or sensitive. It is the sponsor's responsibility to fully and clearly identify the proprietary or sensitive information, to ensure all legal rights to the TOE and related material have been obtained, and to sign the appropriate non-disclosure agreement with the CCTL.

During the course of an evaluation, information about the sponsor's IT product may be shared between the CCTL and NIAP staff. No restrictions shall be placed on information shared between these organizations. As a condition of employment with NIAP, all employees must sign a Statement of Personal Responsibility for Non-Disclosure of Proprietary Information confirming their agreement to protect proprietary/sensitive information. Each CCTL also enters into a Non-Disclosure Agreement with NIAP (see Publication #4 for the sample NDA).

4.1.8.2 Public Information

As a condition of a validation, certain types of information are made available to the public. The VR, ST and the PCL entry are examples of publicly available information. The sponsor must review and agree in writing to the release of information before it is

publicly posted. The sponsor must notify NIAP in writing when entering into a validation agreement if the sponsor does not wish to have a Compliant Product listed on the PCL or the CC Portal. If a compliant product is not listed on the CC Portal, then the product is not considered mutually recognized under the CCRA.

Any requests to NIAP for information about the sponsor's product or evaluation involving information beyond that which is publicly available will be forwarded to the sponsor.

4.1.9 Sponsor Responsibilities

Prior to the start of the evaluation (Phase I), the sponsor is expected to:

a) contract with the CCTL for the conduct of the evaluation, making clear the nature of the evaluation;
b) coordinate with the CCTL to produce an agreed upon evaluation work plan and schedule;
c) commit to the CCTL to fulfill the sponsor role;
d) secure all legal rights to the TOE and to indemnify the CCTL and NIAP in this area;
e) ensure the CCTL submits and gains acceptance of the evaluation into the scheme;
f) ensure the CCTL submits a copy of all required documentation to NIAP;
g) agree not to make any statements in press releases or any other promotional material that might misrepresent the conclusions of the evaluation;
h) participate in meetings with the CCTL and NIAP, as required;
i) obtain the **written** consent of the TOE developer regarding the conditions for limiting access to proprietary information associated with the TOE;
j) give permission for the future release of evaluation results including extracts from evaluation technical reports that are relevant to Common Criteria certificate maintenance activities; and
k) approve listing to PCL and in-evaluation list.

4.1.10 Sponsor's Expectations of the CCTL

During Phase I, the sponsor can expect the CCTL will:

a) be knowledgeable of the CC, NIAP procedures and policies, and the specific technology being evaluated;
b) notify NIAP of the intent to perform an evaluation under the scheme; and
c) facilitate information flow between the sponsor and NIAP.

4.1.11 Sponsor's Expectations of NIAP

During Phase I, the sponsor can expect that NIAP will:

a) coordinate with the CCTL to achieve an acceptable evaluation work schedule; and
b) officially accept the TOE into evaluation for scheme validation and if unable to do so, provide to the CCTL and the sponsor a written rationale for a decision not to accept.

4.2 Phase II

Phase II begins at the Check-In meeting and concludes once a Check In receives a passing verdict.

4.2.1 Sponsor's Responsibilities

During Phase II, it is the responsibility of the sponsor to:

a) inform the CCTL of any changes to the TOE which may affect the security evaluation;
b) answer any questions from the CCTL arising from the analysis of the ST or other evaluation deliverables;
c) provide the CCTL (and NIAP, as required) with detailed proposals for resolving problems arising during the course of evaluation;
d) provide the CCTL with a schedule for the delivery of all evidence necessary to conduct the evaluation;
e) provide access to an appropriate facility where the TOE can be installed and tested in the evaluated configuration; and
f) provide general support to evaluators and validation personnel, including training and access to the developer's staff for technical discussions about the product.

4.2.2 Sponsor's Expectations of CCTL during Phase II

The CCTL is expected to:

a) conduct the evaluation in accordance with the requirements of the contract between the sponsor and the CCTL;
b) provide the sponsor with the opportunity to correct deficiencies in the ST/TOE in lieu of evaluation failure;
c) coordinate with NIAP (Validator) during the evaluation;
d) issue timely observation reports as required;
e) produce an Evaluation Technical Report (ETR) and documentation as required in the CICO guide;
f) facilitate information flow between the sponsor and NIAP;
g) be fully aware of all CC and Assurance Activity interpretations and policy/procedures impacting the evaluation.

4.2.3 Sponsor's Expectations of Validator during Phase II

NIAP (Validator) is expected to:

a) coordinate with the CCTL;
b) issue timely observation decisions in response to CCTL generated observation reports;
c) be knowledgeable of the CC and NIAP procedures and policies, and the specific technology being evaluated;
d) clearly indicate to the sponsor and CCTL which interpretations are to be applied to the evaluation; and

e) provide the sponsor with a NIAP point of contact.

4.2.4 Complaints and Appeals

NIAP provides a process for addressing complaints and appeals. The NIAP Director is responsible for ensuring all complaints and appeals are responded to promptly and corrective action, if required, is implemented. For more details about the Complaint and Appeal process, refer to Publication #2, *Quality Manual and Standard Operating Procedures*.

4.3 Phase III

Phase III starts after completion of the Check In, includes the CCTL delivery of all evaluation documentation to the Validator, and ends with certificate issuance and PCL posting.

4.3.1 Certificate Issuance

Upon completion of Phase II, the CCTL will provide the Validator with the final ST and Evaluation Technical Report (ETR, as defined by the CEM), all evaluation questions to the Technical Rapid Response Team (TRRT) and Evaluation Consistency Review (ECR) team, a draft PCL entry, a draft Validation Report (VR), and any additional documentation detailed in the CICO Guide. The ETR should be complete, including proprietary and/or sensitive information. The format and content requirements for the ETR are provided on the NIAP website at: http://www.niap-ccevs.org/Documents_and_Guidance/forms.cfm.

After a review of all information, the validator will complete the VR. The VR and PCL entry will concurrently be submitted to the sponsor and CCTL for accuracy and release approval. The validator will submit the final package (ST, VR, PCL entry, & ETR) to NIAP for review and approval decision.

The NIAP Director will make the decision to either:

1) prepare a Common Criteria Certificate and forward for signature, issue a PCL entry, and notify our Common Criteria partners for mutual recognition; or

2) notify the CCTL and Sponsor of the unsuccessful completion of the evaluation and the rationale for this decision.

The contents of a CC certificate are described in Publication #1, *Organization, Management and Concept of Operations*.

NIAP notifies the CCRA partners of the certificate issuance and they are provided with the same information that is published in the PCL. The PCL is a summary of certificate information for all Compliant Products.

CCRA partners and vendors are afforded the opportunity to request their product to be placed on the NIAP's Product Compliant List if the following criteria are met:

- Product claimed exact compliance against a NIAP-Approved Protection Profile; and
- The Security Target and Validation report are submitted to NIAP for consistency review.
    - Preferably all publically available documentation will be submitted, but only the Security Target and Validation Report are required.

The purpose of the above criteria is to ensure evaluations of Information Technology (IT) products are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products. In addition, the above criteria assists us in improving the availability of evaluated, security-enhanced IT products while also eliminating the burden of duplicating evaluations of IT products. Furthermore, we strive to continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation process for IT products.

4.3.2 Evaluation Records Management

All records pertaining to an evaluation will be kept by the Scheme for at least five years after the completion of the evaluation. This includes all records and other papers produced in connection with each evaluation. After the archive period has expired, all non-proprietary records supporting an evaluation will be destroyed.

4.3.3 Sponsor Responsibilities Pertaining to Phase III

It is the responsibility of the sponsor:

a) to accept the conclusions in the Validation Report;
b) to review the VR, PCL and certificate and provide the CCTL and NIAP with all required final forms (F8002, F8003, F8004) found at http://www.niap-ccevs.org/Documents_and_Guidance/forms.cfm.

4.4 Phase IV

Once a certificate is issued, NIAP validation activities are completed. However, Assurance Continuity and Certificate monitoring are additional activities requiring NIAP oversight.

4.4.1 Common Criteria Certificate Maintenance

NIAP provides an opportunity for sponsors of security evaluations to maximize previous evaluation results and to cost-effectively continue to participate in the evaluation and validation processes over time. Procedures for the maintenance of Common Criteria certificates are outlined in Publication #6, *Assurance Continuity: Guidance for Maintenance and Re-evaluation*

4.4.2 Certificate use monitoring

NIAP will monitor the use of CC certificates for each NIAP Compliant Product to verify all rules associated with the use of the certificates are followed. The rules governing the use of CC certificates can be found in Publication #2, *Quality Manual and Standard Operating Procedures*.

In addition, the policy regarding the use of the certificate mark is described in Annex D of this publication.

4.4.3 Sponsor responsibilities during Phase IV

During phase IV, the sponsor is expected to:

c) inform NIAP of any factors possibly invalidating the certificate;
d) advertise and market an IT product as a Compliant Product only on the basis of a valid Common Criteria certificate;
e) ensure maintenance of the Common Criteria certificate by complying with the change control requirements specified in the ST, Evaluation Technical Report, or Validation Report for proposed changes to the TOE; and
f) retain all evaluation deliverable change information and related test evidence for potential use in future evaluations.

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 17065:2012 — 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
CICO	Check-In/Check-Out
ECR	Evaluation Consistency Review
ETR	Evaluation Technical Report
ISO	International Organization for Standardization
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
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TRRT	Technical Rapid Response Team
VID	Validation Identification
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 NIAP 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 NIAP-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.

Check-In/Check Out: The process for NIAP to provide validation oversight and to ensure the technical quality of evaluations. Sync Sessions may be conducted if the Validators deem they are appropriate for the given circumstance. Sync Sessions occur on an as needed basis. For more information, please refer to the CICO Guide.

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 NIAP which confirms that and 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 NIAP 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 NIAP 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 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 National Information Assurance Partnership (NIAP).

National Institute of Standards and Technology (NIST): The federal technology agency that works with industry to develop and apply technology, measurements, and standards.

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

Product Compliant List (PCL): A publicly available listing maintained by NIAP Scheme of every IT product/system that has been issued a Common Criteria certificate by NIAP.

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.

Sync Session: A meeting initiated by the Validator that affords the evaluators a chance to clear up issues found in the Check-In meeting. Sync Sessions are not mandatory and occur on an as needed basis.

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 NIAP.

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

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

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

Annex D: Common Criteria Certification Mark Policy

The Common Criteria Certification Mark may be used by vendors in conjunction with advertising, marketing, and selling of their Common Criteria compliant product. "Compliant Product" means only products that have successfully completed evaluation in accordance with the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) Validation Body procedures, have been issued a Common Criteria Certificate by NIAP and are listed on the NIAP Product Compliant List (PCL).

Potential Uses for the Certification Mark

Products & Packaging
The Certification Mark may be used on validated products and validated product packaging.

Brochures/Websites
The Certification Mark may be used by vendors in marketing/sale brochures and websites. If the Certification Mark appears at the top or bottom of a page, all text and graphics appearing on the same page as the logo must refer ONLY to the compliant product. The specific version number, as listed on the Product Compliant List, must be included in either case.

If the Certification Mark appears adjacent to a specific paragraph, all text and graphics in and near that paragraph must refer ONLY to the compliant product. The version number, as listed on the PCL, must be included.

Signs, Trade Show Backdrops, etc.
Only the compliant product (the actual product, a replica, or a picture) may be displayed near the Certification Mark. All literature near the Certification Mark may only refer to the compliant product. The compliant product name and version number, as listed on the PCL, must be included on the sign, banner, backdrop, etc., so it is clear the logo refers to the compliant product.

Scheme Point of Contact
For general information about the Certification Mark use, vendors should contact the NIAP Common Criteria Evaluation and Validation Scheme at 410-854-4458. Prior to initial use of the Certification Mark please provide the scheme point of contact a copy of how you plan to use the certification mark.

NOTE: Vendors cannot alter the certification mark in any way except for size and monochromatic color schemes. Misuse of the Certification Mark may result in legal action.