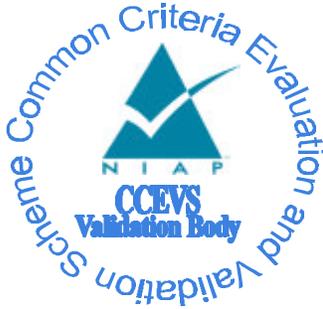


DRAFT - for Review and Comments



Common Criteria
Evaluation and Validation Scheme
for
Information Technology Security

Guidance to CCEVS Approved Common Criteria Testing Laboratories

Scheme Publication #4

Version 1

March 20, 2001

Please submit comments to ccevs-comments@nist.gov

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive, Stop 893
Gaithersburg, MD 20899-8930

National Security Agency
Information Systems Security Organization
9800 Savage Road
Fort George G. Meade, MD 20755

20 March 2001

Version 1.0 Draft

DRAFT - for Review and Comments

This page intentionally left blank

DRAFT - for Review and Comments

1	Introduction	1
1.1	Background	1
1.2	Purpose	2
1.3	Organization of this Document	3
1.4	References	3
1.5	Document Maintenance	4
2	Common Criteria Testing Laboratory	5
2.1	Requirements for CCTL Approval	5
2.1.1	CCEVS-Specific Requirements	5
2.1.2	NVLAP Accreditation	6
2.2	Extending or Reducing CCTL Scope of Accreditation	7
2.3	Renewal of Approval/Accreditation	7
2.4	Withdrawal or Suspension of Approval/Accreditation	8
2.5	Audits	9
2.6	Notifying CCEVS of CCTL operation changes	9
2.7	Evaluation of Assurance Levels (EALs) 5 through 7	9
3	Responsibilities of a CCTL during Pre-Evaluation	11
3.1	Independence and Conflict of Interest	12
3.1.1	CCEVS Conflict of Interest Guidelines	12
3.1.2	Preparation for IT Security Evaluation	13
3.2	Pre-Validation Process	13
3.2.1	Submitting an Evaluation for Acceptance into the Scheme	14
3.2.2	Evaluation Workplan	14
3.2.3	Scheme Resource Assignment	15
3.2.4	Evaluation Kick-off Meeting and Acceptance Agreement	15
4	Responsibilities of a CCTL during Evaluation	17
4.1	Government Roles	18
4.1.1	Government Evaluators	18
4.1.2	Validators	19
4.2	Record Keeping	19
4.3	Observation Reports and Decisions	20
4.3.1	Submission of Observation Reports	20
4.3.2	Handling of Observation Reports	22
4.3.3	Observation Decisions	22
4.4	CC, CEM & CCEVS Process Interpretations	23
5	Responsibilities of a CCTL during Post-Evaluation	24
Annex A.	Glossary of Terms	26
Annex B.	Scheme Publications	32
Annex C.	CCEVS Contact Information	34
Annex D.	Sample Observation Report Format	35
Annex E.	Validation Report Format	36
Annex F.	CCEVS Evaluation Workplan Template	40
Annex G.	Evaluation Acceptance Agreement	43
Annex H.	Sponsor's Approval to List Products that are in Evaluation	47
Annex I.	Sample Kick-off Meeting Agenda	49
Annex J.	Common Criteria Certification Mark Policy	50
Annex K.	Evaluation Technical Report Outline for a Target of Evaluation	51
Annex L.	Evaluation Technical Report Outline for a Protection Profile	58

1 Introduction

The Common Criteria Evaluation and Validation Scheme (CCEVS) for Information Technology Security was established by the National Information Assurance Partnership (NIAP), a partnership established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to evaluate conformance of Information Technology (IT) products and specifications (protection profiles) to international standards. Currently, the CCEVS scope covers information technology products and protection profiles evaluated against the *Common Criteria for Information Technology Security Evaluation* (CC) at Evaluation Assurance Levels (EAL) 1 through 4. The principal participants in the program are the Sponsors of IT product or protection profile evaluations, the product or protection profile developer, the Common Criteria Testing Laboratories (CCTLs) and the CCEVS Validation Body.

A Sponsor is the party requesting and paying for the security evaluation of an IT product or protection profile (PP) conducted by a CCTL. The Sponsor may be the developer of a protection profile, the developer of a product, a value-added reseller of a product, or another party that wishes to have a product evaluated.

A CCTL is a commercial testing laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to perform security evaluations against the *Common Criteria for Information Technology Security Evaluation* (CC) using the *Common Evaluation Methodology for Information Technology Security Evaluation* (CEM).

The CCEVS Validation Body, hereafter referred to as the Validation Body, is the government organization established by the NIAP to implement and operate the evaluation scheme for the U.S. government. This document, the fourth in a series of CCEVS publications, provides guidance to a Common Criteria Testing Laboratory (CCTL) participating in the U.S. Government's evaluation scheme.

1.1 Background

The CC is a set of functional and assurance IT security requirements that was developed by the governments of the United States, Canada, France, Germany, the Netherlands, and the United Kingdom. The purpose of the CC is to provide a common international language in which to express IT security requirements. The CEM was also jointly developed by the same countries to establish a common

DRAFT - for Review and Comments

approach for conducting IT security evaluations against the CC. The ultimate goal of these efforts is to have the results of an evaluation performed by one participating country recognized by another participating country without the product having to be evaluated and certified/validated again.

On October 5, 1998, the initial *Common Criteria Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of Information Technology Security* (CCRA) was signed by the United States, Canada, France, Germany, and the United Kingdom to affirm their commitment to this goal. Both NIST and NSA signed the CCRA on behalf of the United States. In October 1999, Australia and New Zealand joined the Mutual Recognition Arrangement increasing the total number of participating nations to seven. In May 2000 the arrangement was expanded and renamed to the *Common Criteria Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security* (CCRA). The expanded CCRA allowed for the participation of both certificate-consuming and certificate-producing nations, and expanded the number of participating nations to thirteen, which included the United States, Canada, France, Germany, the United Kingdom, Australia, New Zealand, Italy, Spain, the Netherlands, Norway, Finland, and Greece.

The CCRA identifies several conditions necessary for mutual recognition that include use of the CC and CEM as the basis for evaluation criteria and evaluation methods respectively, minimum requirements for Certification/Validation Reports, and the existence of a national Evaluation and Certification/Validation Scheme. To further the goal of achieving consistent, credible and competent application of the CC and CEM, the CCRA also requires the Validation Body to monitor all evaluations in progress within its Scheme. It also requires the Validation Body to establish procedures to ensure that Validation Body and the CCTLS affiliated with the Validation Body perform evaluations impartially; apply the CC and CEM correctly and consistently; and adequately protect the confidentiality of proprietary or sensitive information.

1.2 Purpose

The primary audience of this document is a CCTL and commercial organizations considering becoming a CCTL. The document will help the CCTL personnel prepare for and understand the role of a CCTL prior to, during, and after an IT product/system or PP evaluation. This document will help the CCTL personnel understand and use the CCEVS validation services. Others that may find it useful include product developers and sponsoring organizations.

DRAFT - for Review and Comments

1.3 Organization of this Document

This document consists of the following six chapters and nine Annexes that provide clarifications and guidance to CCTLs participating in the U.S. Government's evaluation scheme.

- Chapter 1 provides the background and context of the Validation Body.
- Chapter 2 provides the requirements for a prospective CCTL.
- Chapter 3 describes the responsibilities of the CCTL prior to conducting an evaluation (pre-evaluation).
- Chapter 4 describes the responsibilities of the CCTL during an evaluation.
- Chapter 5 describes the responsibilities of the CCTL after an evaluation (post-evaluation).
- Chapter 6 discusses the uses and function of the Observation Report
- Annex A contains a Glossary of Terms
- Annex B contains a list of CCEVS publications
- Annex C provides CCEVS contact information
- Annex D identifies Observation Report format
- Annex E identifies the Validation Report format
- Annex F contains the CCEVS Evaluation Workplan format
- Annex G provides a sample Evaluation Acceptance Agreement
- Annex H contains a sample Sponsor's Approval Agreement to List Products that are in Evaluation
- Annex I provides a sample Kick-off Meeting agenda
- Annex J provides CCEVS policy for use of the Common Criteria Certification mark
- Annex K contains the outline for an Evaluation Technical Report for a Target of Evaluation
- Annex L contains the outline for an Evaluation Technical Report for a Protection Profile

1.4 References

Scheme Publication #1, *Common Criteria Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations*, Version 2.0, dated May 1999.

DRAFT - for Review and Comments

Scheme Publication #2, *Common Criteria Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures*, DRAFT, Version 1.5 dated May 2000.

Common Criteria for Information Technology Security Evaluation, Version 2.1, dated August 1999.

Common Evaluation Methodology for Information Technology Security Evaluation, Version 1.0, CEM 99/045, dated August 1999

Common Criteria Arrangement on the Recognition of the Common Criteria Certificates in the Field of Information Technology Security, dated May 2000

NIST Handbook 150, *Procedures and General Requirements*, dated March 1994

NIST Handbook 150-20, *Information Technology Security Testing—Common Criteria Draft*, Version 1.1, dated April 1999

1.5 Document Maintenance

The Validation Body maintains this document, as well as the other documents issued by the CCEVS. Page changes, addendum, or updated versions will be posted to the CCEVS website at the location indicated in Annex C.

2 Common Criteria Testing Laboratory

Organizations interested in becoming a CCTL must go through a series of steps that involve both the NIAP CCEVS Validation Body and the NVLAP. Rather than develop its own accreditation capabilities, the Validation Body has delegated the responsibility of CCTL accreditation to NVLAP. Accreditation by NVLAP is the primary requirement for achieving CCTL status. The NIAP CCEVS Validation Body addresses scheme requirements that cannot be satisfied by NVLAP accreditation. A testing laboratory becomes a CCTL when the laboratory is approved by the Validation Body and is listed on the NIAP CCEVS Approved Laboratories List.

The Validation Body has responsibility for the oversight of evaluations performed by CCTLs within the CCEVS. In performing this oversight, the Validation Body grants approval for a candidate CCTL to become an approved CCTL, modifies approval, coordinates with NVLAP to conduct audits, performs validator observations, and develops and maintains test methods and proficiency tests. The procedures for each of these are addressed below.

2.1 Requirements for CCTL Approval

The Validation Body grants approval for candidate CCTLs to become a CCEVS CCTL when all NIAP CCEVS-specific and NVLAP accreditation requirements have been successfully met. Once all requirements have been met, the candidate CCTL is approved by the Validation Body to conduct IT security evaluations for the specific test methods of its NVLAP accreditation and is placed on the CCEVS Approved Laboratories List.

2.1.1 CCEVS-Specific Requirements

The Validation Body imposes three CCEVS-specific requirements¹:

- a) A CCTL must reside within the U.S. and be a non-governmental legal entity, duly organized and incorporated, validly existing, and in good standing under the laws of the state where the CCTL intends to do business;²

¹ The Validation Body reserves the right to levy additional CCEVS-specific requirements (either technical or administrative), as necessary, when deemed to be in the best interest of the U.S. Government and overall evaluation and validation effort.

DRAFT - for Review and Comments

- b) a CCTL must agree to accept U.S. Government technical oversight and validation of evaluation-related activities in accordance with the policies and procedures established by the CCEVS;
- c) a CCTL must agree to accept U.S. Government participants in NIAP-selected CC evaluations conducted by the CCTL in accordance with the policies and procedures established by the CCEVS; and
- d) a CCTL must be a third party independent evaluation facility.

The Validation Body will:

1. verify the satisfaction of these requirements by inspecting the "Letter of Intent" submitted by a candidate CCTL (See Scheme Publication #1, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Organization, Management, and Concept of Operations*, Annex H for a sample Letter of Intent);
2. document the findings of their verification and place the findings in Validation Body document and records control for a period of five years;
3. notify the candidate CCTL of its findings;
4. notify the CCTL of acceptance as a NIAP CCEVS Approved CCTL when all CCEVS-Specific requirements, and all NVLAP accreditation requirements have been met; and
5. document an agreement with the NIAP CCEVS Approved CCTL.

2.1.2 NVLAP Accreditation

NVLAP accreditation requires a candidate CCTL to demonstrate compliance with general technical and methodological criteria to conduct security evaluations of IT products. NVLAP will follow all instructions and requirements in the following documents to accredit a candidate CCTL:

² Assuming all other U.S. laws and regulatory requirements have been met, a foreign-owned enterprise could establish a testing laboratory in the U.S., become accredited under NVLAP, and be approved by NIAP as a CCTL. However, in order to meet the letter and spirit of the CCEVS requirements, a foreign-owned laboratory must maintain a substantial presence within the U.S., (i.e., a demonstrated, fully operational security testing capability) and all validation activities must be conducted from the U.S. facility.

DRAFT - for Review and Comments

1. NIST Handbook 150³, *Procedures and General Requirements*
2. NIST Handbook 150-20, *Information Technology Security Testing—Common Criteria*

NVLAP issues two documents to candidate CCTLs that have been granted NVLAP accreditation: a Certificate of Accreditation and a Scope of Accreditation. Samples of NVLAP accreditation documents and the steps to becoming accredited are described in Handbook 150-20, Sec. 285.23.

2.2 Extending or Reducing CCTL Scope of Accreditation

A NVLAP scope of accreditation is defined to be the specific *test methods* the CCTL has been accredited to use in conducting IT security evaluations. A candidate CCTL will choose the test methods it wishes to become accredited for from the CCEVS Approved Test Methods List that currently consists of ASE, APE, EAL1, EAL2, EAL3, and EAL4. A CCTL must be accredited for ASE, APE, and EAL1 at a minimum.

CCTLs wishing to expand or reduce their scope of accreditation, (i.e., adding or subtracting test methods) must apply to NVLAP for this change.

2.3 Renewal of Approval/Accreditation

A CCTL must ensure that its CCEVS approval and NVLAP accreditation remains current in order to maintain its status as a CCEVS-approved testing laboratory. CCTLs must have their CCEVS-approved status reconfirmed yearly and their NVLAP accreditation status reconfirmed in accordance with NVLAP procedures. NVLAP procedures typically require reconfirmation to be performed annually, with an on-site assessment occurring every two years. Failure to retain CCEVS approval or NVLAP accreditation will result in withdrawal of the CCTL from the NIAP Approved Laboratories List. As noted in Section 2.2, these procedures will also be followed for a CCTL that has requested either an extension or reduction of accreditation.

The Validation Body will provide the CCTL with a written description of the conditions and steps for renewal. This notification will be delivered 60 days before the renewal date.

³ NIST 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.

DRAFT - for Review and Comments

If a CCTL satisfies the conditions for re-approval/re-accreditation (or extension/reduction of accreditation) the Validation Body will notify the CCTL accordingly and retain the CCTL on the NIAP CCEVS Approved Laboratories List.

If a CCTL fails to respond to the notification or has responded to the notification and fails re-approval/re-accreditation (or extension/reduction of accreditation), the provisions for withdrawal or suspension of approval/accreditation are applied as described in Section 2.4.

2.4 *Withdrawal or Suspension of Approval/Accreditation*

When the Validation Body determines that a CCTL has not complied with all CCEVS and NVLAP requirements, the CCTL may have its status withdrawn or suspended.

If a CCTL has its CCEVS approval or NVLAP accreditation *withdrawn* the CCTL must cease all CCEVS evaluation activities, is removed from the NIAP Approved Laboratories List, and must reapply for approval or accreditation as a CCTL.

If a CCTL has its CCEVS approval or NVLAP accreditation *suspended* the CCTL must *temporarily* cease all CCEVS evaluation activities until it resolves the condition(s) that caused the suspension. If the CCTL does not resolve the condition(s) that caused its suspension, its status as a NIAP CCEVS Approved CCTL will be withdrawn.

The conditions for withdrawal and suspension of *CCEVS approval* are described in Scheme Publication #1, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Organization, Management, and Concept of Operations*, Annex C.

The conditions for withdrawal and suspension of *NVLAP accreditation* are described in NIST Handbooks 150 and 150-20.

When the Validation Body determines that a CCTL should be withdrawn or suspended it will notify a CCTL in writing 30 days before withdrawal or suspension date. The notification from the Validation Body will provide the CCTL with a description of the reason(s) for withdrawal or suspension and steps to follow to regain its status as a CCTL. If a CCTL fails to respond to the notification or comply with the notification, the Validation Body will:

DRAFT - for Review and Comments

1. provide written notification to the CCTL that they are no longer an approved CCTL;
2. provide written notification to all sponsors of evaluations the CCTL is currently performing, that the CCTL is no longer an approved CCTL; and
3. withdraw all resources from evaluations associated with the CCTL and remove it from the *NIAP Approved Laboratories List*.

2.5 Audits

NVLAP or the Validation Body may audit a CCTL to ensure that the CCEVS requirements continue to be met. The Validation Body will follow its internal auditing procedures during a CCTL audit (see Scheme Publication #2, Section 4.4). NVLAP will follow NIST Handbook 150 for its audit procedures. Auditing by either NVLAP or the Validation Body will be coordinated between them such that conflicts and duplication do not occur.

CCTLs are required to define and maintain procedures for internal audits, and provide the results of the internal audits to the Validation Body and NVLAP upon request. CCTLs are also required to inform the Validation Body in writing of any changes in its status that may cause it to violate a CCEVS requirement, e.g., change in ownership, or NVLAP accreditation requirement.

2.6 Notifying CCEVS of CCTL operation changes

A CCTL must notify Scheme management in writing if there are any significant changes in CCTL operations from what was described in the Letter of Intent or from what was the basis for NVLAP accreditation. Examples of events that require written notification are a CCTL's intent to withdraw from the Scheme, changes in ownership of a CCTL, or personnel changes in key staff positions. The above-listed examples provide guidance on the types of changes that require written notification, but this list is not all-inclusive. A CCTL should contact the Scheme if there is a question about whether a change is significant enough to warrant written notification.

2.7 Evaluation of Assurance Levels (EALs) 5 through 7

Currently, the major scope of the CEM and CCEVS procedures and guidelines focuses on evaluating information technology products and protection profiles

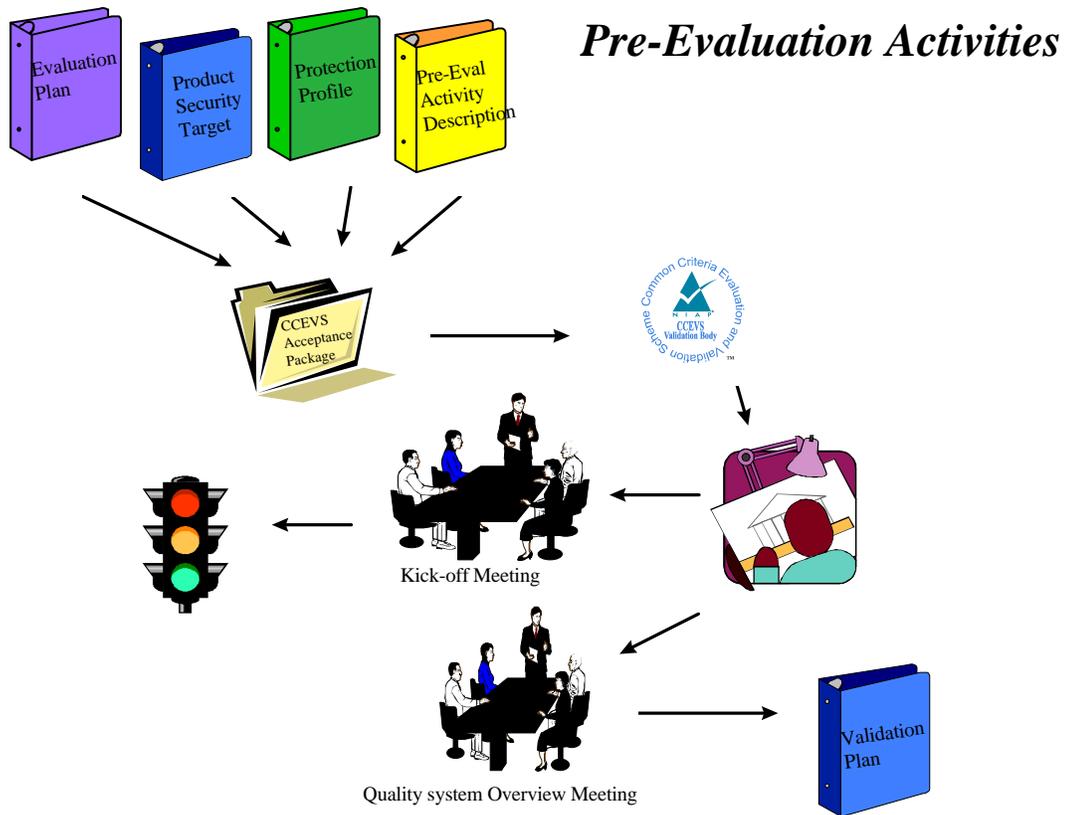
DRAFT - for Review and Comments

against the *Common Criteria for Information Technology Security Evaluation* (CC) at Evaluation Assurance Levels (EAL) 1 through 4. Because there is little agreed upon CEM guidance for CC evaluations above EAL 4, the current CCRA only provides mutual recognition of certifications/validations at EAL 1 through 4. Certifications/validations at EAL 5 and above are currently not recognized under the CCRA.

Nevertheless, sponsors and CCTLs are encouraged to work in partnership with the Validation Body in conducting evaluations at EAL 5 and above. The Validation Body will work with sponsors and CCTLs on a case-by-case basis in assessing those CC components above EAL 4. Depending on the technology and the circumstances, the U.S. Government may opt to have Government Evaluators accomplish the tasks and provide the results to the CCTL, may choose to augment CCTL's team with Government Evaluators, may provide supplemental evaluation methodology and have the CCTL conduct the evaluation, or any combination of the above.

Successfully completed evaluations at EAL5-7 will be posted to the VPL with the caveat that some components are above EAL4 and therefore are beyond the scope of the CCRA.

3 Responsibilities of a CCTL during Pre-Evaluation



This chapter provides guidance that is relevant to CCTLs prior to starting an evaluation.

The period of *pre-evaluation* is considered to be any evaluation/validation-related activity that occurs prior to the signing of agreements between the sponsor/CCTL/Validation Body for the evaluation/validation.

An *evaluation* commences once the agreements are signed and ends just prior to the issuance of the Validated Products List entry.

DRAFT - for Review and Comments

Post-evaluation commences with the publication of the Validated Products List entry and the issuance of the certificate.

3.1 Independence and Conflict of Interest

NIAP CCTLs will conduct third party independent evaluation of products and PPs. CCTLs must observe the highest standards of impartiality, integrity, and commercial confidentiality, and operate within the guidelines established by the scheme. CCTLs must follow documented policies and procedures in order to ensure the protection of sensitive or proprietary information. These procedures shall be subject to audit by the NVLAP and the NIAP CCEVS Validation Body.

3.1.1 CCEVS Conflict of Interest Guidelines

Neither the CCTL, its parent corporation, nor any individual CCTL staff member 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 evaluation of an IT product or Protection Profile; or
- b) providing consulting services that would compromise the independence of the evaluation to the sponsor of an evaluation or to the product/PP developer.

Accordingly, CCTLs must ensure that any activities related to the production of evaluation evidence in preparation for the evaluation (within that same testing laboratory) of an IT product or PP do not conflict with the laboratory's ability to conduct a fair and impartial evaluation of that product or profile. 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 that the advice given does not affect evaluator independence or impartiality in any evaluation. The CCTL must notify the CCEVS whenever any potential conflict of interest may occur. All CCTLs will be subject to the conflict of interest guidelines stated above. The NIAP CCEVS Validation Body and NVLAP will verify that these conditions are met and will be the final arbitrators in determining potential or actual conflicts of interest that may threaten the integrity of security evaluations conducted within the scheme.

DRAFT - for Review and Comments

3.1.2 Preparation for IT Security Evaluation

The majority of pre-evaluation activity occurs between the CCTL and the sponsor of the evaluation. The sponsor is responsible for providing the protection profile (PP) or the security target (ST) and the associated IT product/system that will become the 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 CCTL must ensure that arrangements have been made with the evaluation sponsor for the provision of all essential documentation to the CCTL evaluation team in order to conduct a successful security evaluation.

If a CCTL is used for both consulting and evaluation, contract negotiations between the CCTL and the sponsor should clearly specify that different CCTL personnel must be used for the two different functions. The Validation Body leaves details of the contract between the CCTL and the sponsor to the two parties to negotiate, with no involvement.

3.2 Pre-Validation Process

To achieve oversight activities, the scheme will employ a validation program that is designed to combine training and practical experience. This will provide the breadth and depth necessary to provide competent validators who will ensure the quality of evaluation results produced by the scheme. An overview of the CCEVS Validation process is described below. Detailed procedures for administering technical oversight and validation are described in Scheme Publication #3, *Common Criteria Evaluation and Validation Scheme for Information Technology Security - Technical Oversight and Validation Procedures*.

A sponsor of an evaluation (e.g., vendor of a product or protection profile developer) interested in obtaining a Common Criteria evaluation through the scheme approaches one or more of the CCEVS authorized CCTLs for evaluation services. Any discussions regarding the price of the evaluation, the nature or conditions of payment, and the schedule for the evaluation are left entirely up to the CCTL and the sponsor of the evaluation. Similarly, proposal content and any screening or pre-investigation that the CCTL may wish to conduct regarding the viability of the protection profile or product is left to the discretion of the CCTL. When entering into an agreement with a customer, the CCTL must ensure that there is no conflict of interest or appearance of conflict of interest in performing an evaluation if the intent is to obtain a Common Criteria Certificate.

DRAFT - for Review and Comments

3.2.1 Submitting an Evaluation for Acceptance into the Scheme

Once the sponsor of the evaluation selects a CCTL and they have an agreement, the CCTL must submit a request to have the evaluation formally accepted into the scheme⁴. In order for a product or system to be accepted into the scheme, the CCTL must submit an Evaluation Acceptance Package (EAP) in triplicate (if hardcopy) or electronically to the Director, CCEVS. The EAP consists of the following:

- 1) a complete Security Target for the Target of Evaluation (TOE),
- 2) a complete Evaluation Workplan for the evaluation (see Annex G for format), and
- 3) a description of the extent and nature of pre-evaluation activity with the sponsor, including the names of the individuals involved.

For a PP evaluation to be accepted into the scheme, the CCTL must submit the following items (Evaluation Acceptance Package) to the Validation Body:

- 1) the complete protection profile,
- 2) a complete Evaluation Workplan for the evaluation, and
- 3) a description of the extent and nature of pre-evaluation activity with the sponsor, including the names of the individuals involved.

3.2.2 Evaluation Workplan

The evaluation team will develop the evaluation workplan prior to the start of the evaluation (see Annex G for a sample Evaluation Workplan outline). This is a critical document for the validator in planning the validation activities. The evaluation workplan describes all the work packages that will be performed during the evaluation, any output that will be produced during the evaluation analysis, and how the work package results will be documented. The evaluation workplan should be written to a level of detail that allows the validator to gain confidence that the lab understands the work required and can describe the methodology that will be used in performing the evaluation.

A detailed evaluation workplan will provide the validator with more insight into the processes and analysis methods that will be used by the evaluation team during the

⁴ While it is envisioned that sponsors of evaluations and CCTLs will enter into an agreement before approaching the CCEVS Validation Body, it is acceptable for the sponsor and/or CCTL to meet with the CCEVS Validation Body prior to entering into a formal agreement to assess the feasibility of conducting an evaluation under the scheme. This pre-acceptance meeting will in no way replace the formal notification process and meeting necessary for formally entering into the scheme.

DRAFT - for Review and Comments

course of the evaluation. The validator can then use the evaluation workplan as input when developing the validation plan. Given a detailed evaluation workplan, the validator can articulate the validation activities with more accuracy. A properly written evaluation workplan also provides the validator with confidence in the lab's ability to define and clearly describe the evaluation methods and analysis.

If the evaluation workplan does not provide the validator with confidence in the lab's ability, then the validator must delve into more detail during the course of the validation. An evaluation workplan with few specific details forces the validator to include extra validation analysis to compensate for the fact that the lab has not used the evaluation workplan to document knowledge of the evaluation analysis and methods required.

A well-written, detailed evaluation workplan is in the best interest of the lab, as it will allow the validator to write a more accurate validation plan and to determine the lab's understanding of the methods and analysis that are required for a given evaluation.

3.2.3 Scheme Resource Assignment

Upon receipt of an EAP from a CCTL, the Validation Body will review the submitted information and identify validation resource needs for the effort. Based on this initial review of the ST or PP, the EAL, and the complexity of the TOE or PP, one or more validation personnel will be assigned and a Lead Validator designated. Additionally, senior validation personnel from the Validation Body will be identified to provide support and guidance to the Validator(s) upon the request of the Validator.

Upon submission of the Evaluation Acceptance Package but prior to official acceptance into the Scheme, the CCTL may choose to begin ASE evaluation work. This decision, which may be made by the CCTL, has two significant risks associated with it. The risks are that the evaluation may not be accepted by the Scheme for various reasons, or the Validation Body may require all scheme procedural steps be done and the evaluation process may need to be re-started from the beginning in order for the Validator(s) to perform their functions.

3.2.4 Evaluation Kick-off Meeting and Acceptance Agreement

Within 8 business days of assignment, the Lead Validator for the evaluation will conduct a complete review of all information and will schedule two meetings: a CCTL Quality System Overview meeting and an Evaluation Kick-off meeting.

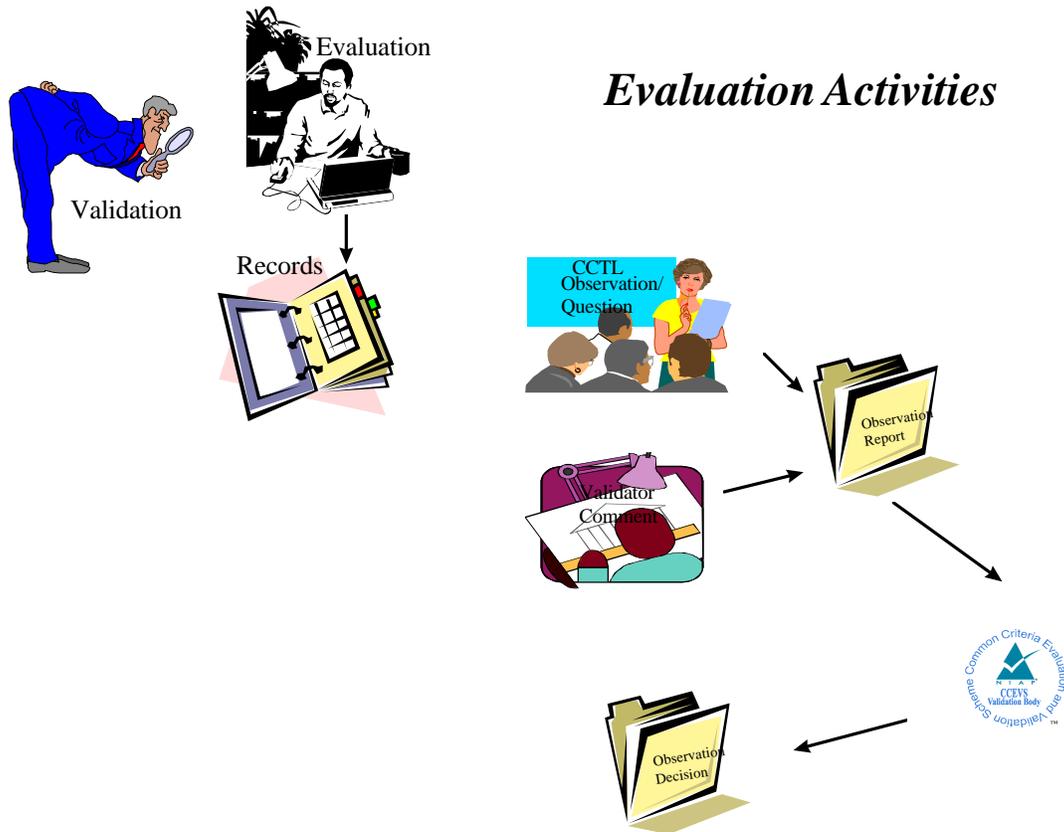
DRAFT - for Review and Comments

The Validation Body management and the assigned validation personnel will conduct an Evaluation Kick-off meeting with the CCTL and Sponsor to review the evaluation plan, identify validation milestones, and generally manage expectations. See Annex J for a sample Kick-off meeting agenda. Once this meeting has occurred and all parties are in agreement, the Validation Body, CCTL, and Sponsor will sign an Evaluation Acceptance Agreement (see Annex H). The Evaluation Acceptance Agreement states that the evaluation has been officially accepted into the scheme and that all evaluation and validation activities can commence.

The CCTL Quality System Overview meeting may be held prior to or following the Kick-off meeting. The purpose of this meeting is to allow the CCTL to provide the validator with background information and a general description of the Quality System. This may include a description of the types of records that will be kept and a sample of actual records. This meeting will give the validator an understanding of the CCTL's quality system, thereby allowing the validator to document the validation activities in the Validation Plan.

Given an understanding of the CCTL's Quality System, and using the ST or PP and the evaluation workplan, the validator will develop a Validation Plan for the evaluation. The Validation Plan will outline the various validation activities, the validation milestones, and their approval authority. The validator will submit the Validation Plan to the CCTL and the Chief Validator within 8 business days of the Quality System Overview meeting.

4 Responsibilities of a CCTL during Evaluation



This chapter provides guidance that is relevant to CCTLs during an evaluation.

The *Evaluation* commences once the agreements are signed and the Evaluation Kick-off has been held, and ends just prior to the issuance of the NIAP Common Criteria Certificate.

After an evaluation has been officially accepted into the scheme, the evaluation and validation activities will commence. The CCTL will conduct all evaluation activities in accordance with the CEM, the evaluation workplan, and CCEVS process. The Validator will concurrently monitor CCTL activities, conduct validation activities in accordance with the validation plan, prepare and submit validation status reports in

DRAFT - for Review and Comments

accordance with the validation plan, coordinate all CCTL generated Observation Reports (ORs) submitted to the Validation Body, and provide a continual interface with the Validation Body.

Upon completion of the evaluation analyses, the CCTL will provide the Validator with all evaluation ORs along with any corresponding Observation Decisions (ODs), a draft Validated Products List Entry Summary, and two versions of the Evaluation Technical Report (ETR). The two versions of the report will be as follows:

1. a complete ETR, including proprietary and/or sensitive information; and
2. an abridged ETR which is a complete report excluding only proprietary and/or sensitive information.

After a detailed review of all information, the Validator will produce a Validation Report and recommendation. The Validation Report and Validated Products List Entry Summary will concurrently be submitted to the CCTL and Sponsor for accuracy and release approval. Validators will provide a final recommendation to the Technical Oversight Manager for concurrence and presentation to the Director of the Validation Body.

4.1 Government Roles

The CCTL will regularly interface with the Government Evaluators(s) (GE) who are evaluators assigned as members of an evaluation team, and with Government Validators who are assigned to oversee an evaluation. This section describes the responsibilities of these two CCEVS representatives.

4.1.1 Government Evaluators

The GE is an individual assigned as a team member on an evaluation. The assignment is made at government discretion in coordination with the CCTL as a training opportunity or for some evaluation-related reason, and the lab cannot decline it. As a member of the evaluation team, the GE can produce a portion of the evaluation results, including analysis, tests, evaluation related records (e.g., documentation required by the CCTL quality system, evaluation specific workplans, or individual work packages), and evaluation report content. Although a government employee (or CCEVS partner), the GE receives evaluation assignments and direction from the CCTL's Team Leader, taking into account the skills, interests, and abilities of the individual.

DRAFT - for Review and Comments

The GE is expected to follow the lab's processes and procedures. The GE should not develop the quality procedures for the lab, but can be required to produce documentary evidence of evaluator actions in accordance with the CCTL quality procedures. GEs are not involved in the performance of Validation activities or in the rendering of any validation recommendation.

CCTLs do not use GEs as a cost saving opportunity. The bids submitted by CCTLs to a potential evaluation sponsor do not depend upon the addition of a GE to an evaluation team. Rather, the CCTLs must accept a GP if offered by the government.

4.1.2 Validators

A Validator is assigned to each evaluation to act as a liaison between the Validation Body and the CCTL and to ensure that the evaluation meets CCEVS standards and satisfies the requirements of the CCRA. The Validator advises the CCTL on both technical and process issues but does not produce evaluation evidence, such as evaluation report sections or test reports. The tasks performed and the degree of involvement in team activities will vary from one evaluation to another, and are likely to increase at higher EALs. Optional activities are at the discretion of the Validator, not of the CCTL. The Validator may participate in team training, observe team meetings, assess lab processes and procedures, and review evaluation evidence.

The primary products of the Validator are the advice given to the team on evaluation issues and the insight given to the Validation body about the evaluation progress. The Validator does not produce evaluation evidence.

Throughout the evaluation, the Validator will produce monthly activity reports, postings to appropriate forums, contributions to the Validator web page, or other communications to record the status and progress of the evaluation, issues, or problems. At the completion of the evaluation, the Validator produces a Validation Report (see Annex F) that summarizes an assessment of the evaluation process and the team.

4.2 Record Keeping

Each CCTL is required to conduct and document evaluations within their Quality System. The establishment and use of the quality system is a requirement for accreditation under NVLAP and approval by the CCEVS. A laboratory is required to submit an evaluation workplan to the CCEVS as part of the acceptance package.

DRAFT - for Review and Comments

The workplan includes a list of CEM work packages that are to be performed during the evaluation. As these work packages are completed, the results are documented and entered as records into the CCTL's quality system.

CCTL records are critical to the validator throughout the course of the validation. The validator gains confidence in the CCTL's ability to define and perform the required analysis for the evaluation by reviewing the records kept throughout the evaluation. The record for each work package must contain both the plan and the results of the work performed. The plan must include the objective of the work package, the required inputs, and the techniques and tools that will be used to perform the work package.

The results of the work package are the complete written analysis or other actions performed by the laboratory to complete the work package, including the rationale and verdict for the work package. Each record must also contain information about the people who performed the work and the dates on which the work was performed.

Complete and thorough records aid the validator in performing the validation. Such records can help provide the validator with confidence in the lab's ability to perform the required analysis correctly. Incomplete or inconsistent record keeping causes the validator to have to perform more detailed or even shadow analysis throughout the course of the evaluation.

4.3 Observation Reports and Decisions

An Observation Report (OR – see Annex D) is a vehicle for the Common Criteria Testing Laboratory (CCTL) to obtain approval of a proposed solution to an observed Common Criteria (CC) technical evaluation issue or scheme process issue (i.e., CCTL question, concern or problem). The CCTL documents in the OR the evaluation or process issue, provides background information and offers a proposed solution. The CCEVS Validation Body uses the OR in reviewing the issue and in developing clarification/guidance to the CCTL. The Validation Body formally responds to the CCTL by issuing an Observation Decision (OD) for each OR.

4.3.1 Submission of Observation Reports

DRAFT - for Review and Comments

The CCTLs should submit an OR when, but not limited to, the:

1. CCTL wishes to apply the criteria to an evaluation where the criteria needs clarification or there are several potential ways to apply the criteria, and no prior documented guidance has been issued by the Validation Body;
2. CCTL wishes to apply the criteria to an evaluation in a way counter to prior documented guidance issued by the Validation Body;
3. CCTL wishes to utilize an evaluation methodology where there are several potentially acceptable methodologies, and no prior documented guidance has been issued by the Validation Body;
4. CCTL is instructed by a validator to submit an OR documenting a decision that the validator believes may be controversial or of general concern; or
5. CCTL could not find a final international or national CC/CEM interpretation or scheme process interpretation on the issue.

A CCTL must submit ORs to the Validator assigned to the evaluation for which the OR was generated.

An Observation Report should contain, at a minimum the:

1. date of submission,
2. projected expiration date when the OR is applicable (current projected evaluation completion date + 6 months),
3. identity of the CCTL submitting the OR,
4. CCTL point of contact for the issue including contact information (e-mail and phone),
5. CCTL specific tracking ID (optional; if desired by the CCTL),
6. identity of the primary Validator for the evaluation including contact information (e-mail and phone),
7. evaluation for which the OR is being submitted,
8. evaluation target (which PP, or EAL for ST),
9. issue for which a resolution is requested,
10. state whether it is a scheme process issue or a technical evaluation issue,
11. proposed resolution to the issue and impact (may include various resolutions and respective impacts),
12. background explanation of the issue and of the proposed resolution, and
13. identification of all information sources (i.e., references) used in preparing the OR.

See Annex D for a Sample Observation Report Format.

DRAFT - for Review and Comments

All information in the OR must be marked by paragraph as either (U) for unclassified or (U//PROPIN) for proprietary information.

4.3.2 Handling of Observation Reports

When the Validator receives the OR he/she:

- verifies that the OR submitted meets the format requirements,
- adds any Validator comments to the background section,
- references any known precedents, prior guidance, ODs or interpretations on the issue,
- issues a receipt of acknowledgement or other means to the CCTL that the OR was received, and
- submits the OR to the Director CCEVS or Technical Oversight Manager as appropriate

The Director CCEVS will coordinate or appoint a coordinator for issues that are primarily scheme process related. The Technical Oversight Manager will coordinate or appoint a coordinator for issues that are primarily technical evaluation related.

Upon receipt of an OR the coordinator will schedule a process and establish an expected date for resolution. Within 3 business days of receipt of the OR the coordinator, working with the Validator, will notify the CCTL that the OR has been received, and provide preliminary information on the process and expected date for the resolution. Upon receipt of an OR, the Validation Body resolution process will usually be accomplished within eight working days.

4.3.3 Observation Decisions

An Observation Decision (OD) is issued in response to an OR. The OD is the formal documented response from the Validation Body that provides clarification/guidance to the CCTL on a submitted OR.

The CCTL is expected to apply the OD:

1. Only for the issue identified in the OR and only for the specific evaluation in question;

DRAFT - for Review and Comments

2. If the associated OR fully disclosed all relevant information that was known or should have been known to the CCTL; and
3. If the evaluation has not exceeded its scheduled completion date by more than six months from the date the OR was submitted.

The Validator works with the CCTL to develop a reasonable proposed resolution and to provide the CCTL with a good-faith understanding of the OD based on the Validation Body's oversight knowledge. The OD is intended to provide the CCTL with confidence that the currently understood resolution will be honored for the evaluation in question when the final validation of evaluation results is conducted.

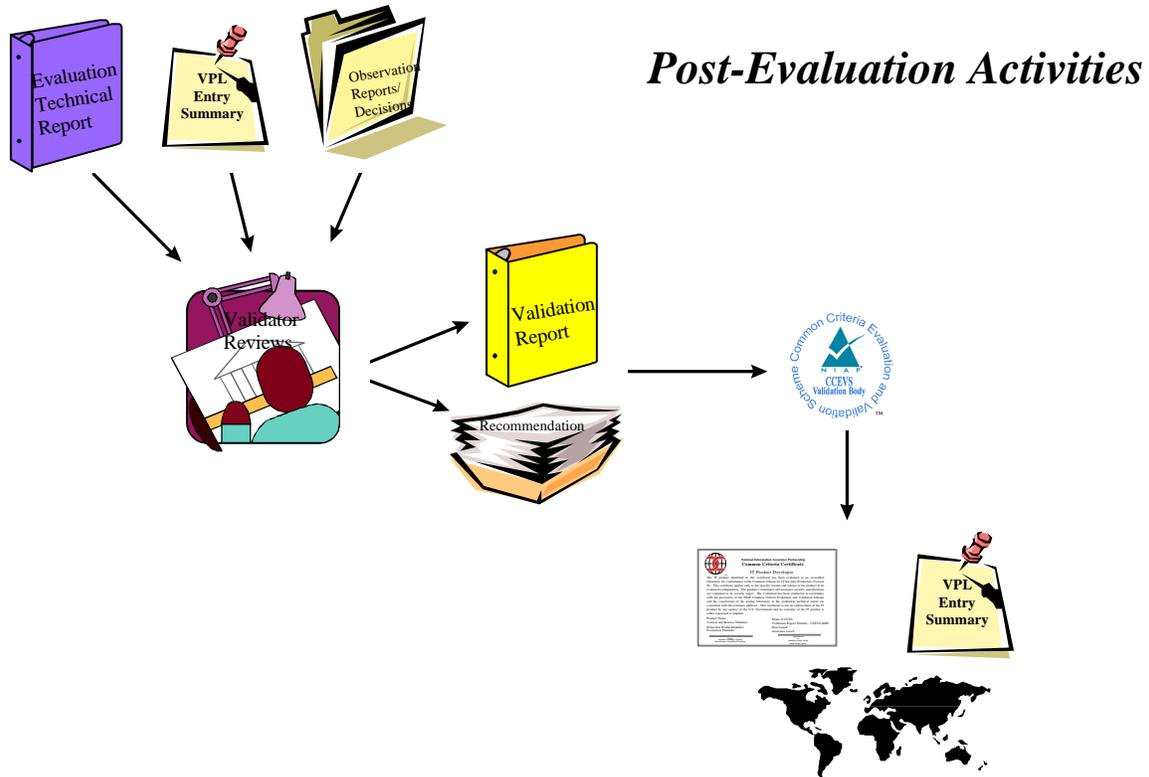
While an OD for a specific evaluation is issued in a very short time-frame to accommodate the CCTL evaluation schedule, this may not provide adequate time for the evaluation oversight community to consider all the implications for all evaluations and produce a completely technically sound, consistent, and widely applicable decision. ODs provide the best answer available at the time for the purpose of giving good-faith guidance to CCTLs on a given evaluation. Even though an OD has been issued on an OR for an evaluation it may not apply to all future evaluations. Thus, the CCTL should resubmit an OR for the same issue for each evaluation to which the issue applies.

4.4 CC, CEM & CCEVS Process Interpretations

A CCEVS Interpretation Board will be used to provide guidance for technical and process issues in CCEVS evaluations. The board receives issues needing clarification or formal interpretation from CCEVS management, validators, or the general public. The interpretation board drafts a proposed statement of technical guidance, and facilitates the scheme and public discussion of draft interpretations to ensure that diverse views are considered. Once all views are considered and incorporated as appropriate, the proposed interpretations are submitted to the Director, CCEVS for approval. Once approved, the interpretations are submitted to the CCIMB for international coordination. The details of the interpretation board operating procedures will be documented in a separate scheme document.

Final national and international criteria interpretations are applicable to an evaluation, effective on the date of acceptance into the Scheme. The CCTL is responsible for ensuring that all applicable interpretations are incorporated as part of the evaluation.

5 Responsibilities of a CCTL during Post-Evaluation



Post-evaluation commences with the publication of the Validated Products List entry and the issuance of the certificate.

Upon completion of the evaluation analyses, the CCTL will provide the Validator with all evaluation ORs along with any corresponding Observation Decisions (ODs), a draft Validated Products List Entry Summary, and two versions of the Evaluation Technical Report (ETR). The two versions of the report will be as follows:

3. a complete ETR, including proprietary and/or sensitive information; and
4. an abridged ETR which is a complete report excluding only proprietary and/or sensitive information.

DRAFT - for Review and Comments

After a review of all information, the validator will produce a validation report and recommendation. The validation report and VPL entry summary will concurrently be submitted to the sponsor and CCTL for accuracy and release approval. The validator will provide a final recommendation to the CCEVS Technical Oversight Manager for concurrence and presentation to the Director of the Validation Body.

Using the final recommendation, the Director of the Validation Body will make the decision to either:

- 1) prepare a Common Criteria Certificate for signature, issue a Validated Products List Entry, and notify our Common Criteria partner schemes for mutual recognition; or
- 2) notify the CCTL and Sponsor of the unsuccessful completion of the evaluation and the rationale for this decision.

Following the decision to issue a CC certificate for a product or PP, the Director of the Validation Body prepares the certificate and rationale for issuing the certificate and forwards them to NSA and NIST signatories. CC certificates are issued to product developers, sponsors, or PP developers on behalf of IT products and PPs that have been evaluated and validated against the CC according to the rules of the CCEVS. To be valid, the certificates must be signed by both the NIST and NSA signatories. The contents of a CC certificate are described in Scheme Publication #1, *Common Criteria Evaluation and Validation Scheme, Organization, Management and Concept of Operations*, Annex E.

There are rules associated with the use of the CCEVS certificates and the CC Certification Mark. See Annex K for the CC Certification Mark Usage Policy.

DRAFT - for Review and Comments

Annex A. Glossary of Terms

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 also broadly consistent with the Common Criteria and Common Methodology. However, the definitions of terms may have been amplified to add greater clarity or to interpret in the context of the evaluations conducted within the scheme.

Accredited: Formally confirmed by an accreditation body as meeting a predetermined standard of impartiality and general technical, methodological, and procedural competence.

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.

Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security (CCRA): An arrangement whereby the Parties (i.e., signatories from participating nations) commit themselves (with respect to IT products and protection profiles) to recognize the Common Criteria certificates issued by any one of them under the terms of the Agreement.

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

Approval Policy: A part of the essential documentation of the Common Criteria Evaluation and Validation Scheme. The policy documents:

1. the procedures for application to become a CCTL;
2. the procedures for a CCTL to be placed on the NIAP Approved Laboratories List;
3. a description of the methods used by NIAP for processing CCTL applications; and
4. the requirements to be met by a CCTL applicant in order to qualify.

Approved: Assessed by the NIAP Validation Body as technically competent in the specific field of IT security evaluation and formally authorized to carry out evaluations within the context of the Common Criteria Evaluation and Validation Scheme.

Approved Laboratories List: The list of approved CCTLs authorized by the NIAP Validation Body to conduct IT security evaluations within the Common Criteria Evaluation and Validation Scheme.

DRAFT - for Review and Comments

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

Assurance Maintenance Plan: Part of the formal assurance maintenance documentation (as part of the initial TOE evaluation) submitted to the Validation Body by the sponsor of an evaluation. The Assurance Maintenance Plan identifies the plans and procedures a developer will implement in order to preserve the assurance obtained in the validated TOE as changes are made to the TOE or its environment.

Availability: The prevention of unauthorized withholding of information resources.

Certificate Maintenance Program: A program within the Common Criteria Scheme that allows a sponsor to maintain a Common Criteria certificate. Certificates are maintained through mechanisms (based on specific assurance maintenance requirements) designed to ensure that a validated TOE will continue to meet its security target as changes are made to the IT product or its environment.

Certificate Maintenance Report: A report prepared by a CCTL for the Validation Body detailing the results of evaluation maintenance activities conducted on behalf of a sponsor.

Certificate Maintenance Summary Report: An annual report prepared by a sponsor for the Validation Body providing a summary of all certificate maintenance activities conducted during the previous year.

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

Common Methodology (CEM): Common Methodology for Information Technology Security Evaluation: a technical document that describes a set of IT security evaluation methods.

Common Criteria Certificate: A brief public document issued by the NIAP Validation Body under the authority of NIST and NSA which confirms that an IT product or protection profile has successfully completed evaluation by a CCTL. A Common Criteria certificate always has an associated validation report.

DRAFT - for Review and Comments

Common Criteria Evaluation and Validation Scheme (CCEVS): The program developed by NIST and NSA as part of the National Information Assurance Partnership (NIAP), establishing an organizational and technical framework to evaluate the trustworthiness of IT products and protection profiles.

Common Criteria Testing Laboratory (CCTL): a non-governmental IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations under CCEVS.

Complaint: a written formal allegation or disagreement against a party.

Complainant: the party initiating a complaint.

Confidentiality: the prevention of unauthorized disclosure of information.

Deliverables List: a document produced by a CCTL containing the list of documents comprising:

1. the security target;
2. all representations of the TOE; and
3. developer support required to conduct an IT security evaluation in accordance with the CCTL's evaluation workplan.

Evaluation: The assessment of an IT product or PP against the CC using the CEM.

Evaluation and Validation Scheme: the systematic organization of the functions of evaluation and validation within a given country under the authority of a Validation Body in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved.

Evaluation Schedule: the schedule established by a CCTL for the conduct of an IT security evaluation.

Evaluation Technical Report: a report detailing the results of an evaluation, submitted by the CCTL to the NIAP Validation Body as the principal input for the validation report.

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

DRAFT - for Review and Comments

Integrity: the prevention of the unauthorized modification of information.

Interpretation: expert technical judgement regarding the meaning or method of application of any technical aspect of the Common Criteria and/or Common Methodology.

IT Product: a package of IT hardware, software, and/or firmware providing functionality designed for standalone use or within an IT system.

IT System: a group of IT products, either tightly or loosely coupled, working together in a specific configuration to provide a capability or system solution to a consumer in response to a stated need.

IT Security Evaluation Criteria: a compilation of the necessary information to be provided and the actions to be taken in order to provide grounds for confidence that security evaluations will be carried out effectively and to a consistent standard.

IT Security Evaluation Methodology: a methodology to be used by evaluation facilities in applying IT security evaluation criteria in order to give grounds for confidence that evaluations will be carried out effectively and to a consistent standard.

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

NIAP Validation Body: a government organization responsible for carrying out validation and for overseeing the day-to-day operation of the CCEVS.

Observation Reports: a report issued to the NIAP Validation Body by a CCTL or sponsor identifying specific problems or issues related to the conduct of an IT security evaluation.

Party: A signatory to the *Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security*.

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

Recognition of Common Criteria Certificates: acknowledgment by one Party of the validity of the Common Criteria certificates issued by another Party based on the

DRAFT - for Review and Comments

Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security.

Scope of Accreditation: the NIAP-approved test methods for which a CCTL has been accredited by NVLAP.

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 ST specifies the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

Sponsor: the person or organization that requests a security evaluation of an IT product or protection profile.

Target of Evaluation (TOE): an IT product/system or PP and the associated documentation that is the subject of a CC evaluation.

Test Method: an evaluation assurance package from the Common Criteria and the associated evaluation methodology for that assurance package from the Common Methodology.

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

Validated Products List (VPL): a publicly available document issued periodically by the NIAP Validation Body. The VPL provides a brief description of every IT product/system or PP that holds a valid CC certificate awarded by either the NIAP Validation or by another Party for which the certificate has been recognized.

Validation Report: a publicly available document issued by the NIAP Validation Body. The validation report summarizes the results of an evaluation and confirms the overall results (i.e., that the evaluation has been properly carried out; that the CC, the CEM, and the scheme-specific procedures have been correctly applied; and that the conclusions of the ETR are consistent with the evidence adduced).

DRAFT - for Review and Comments

DRAFT - for Review and Comments

Annex B. Scheme Publications

The following is a list of CCEVS Publications

Scheme Publication #1 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Organization, Management, and Concept of Operations*

Scheme Publication #2 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Validation Body Standard Operating Procedures*

Scheme Publication #3 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Technical Oversight and Validation Procedures*

Scheme Publication #4 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Guidance to Common Criteria Testing Laboratories*

Scheme Publication #5 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Guidance to Sponsors of IT Security Evaluations*

Scheme Publication #6 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Certificate Maintenance Program*

Validated Products List

Validation Reports

NIAP Approved CCEVS Laboratories List

Validation Body Annual Report

CCEVS Newsletters

Official Notices/Addendum

General information about the CCEVS program

- Information and application for becoming a CCTL
- Information and application for entering the CCEVS

NAVLAP Related Documents

NIST Handbook 150 *Procedures and General Requirements*

DRAFT - for Review and Comments

NIST Handbook 150-20 *Information Technology Security Testing—Common
Criteria*

DRAFT - for Review and Comments

Annex C. CCEVS Contact Information

Public information about the CCEVS may be retrieved from the NIAP Web site at <http://niap.nist.gov/cc-scheme> or can be requested by phone or mail. Phone inquiries may be made to **301-975-3247**. Mail inquiries may be directed to:

Director
Common Criteria Evaluation & Validation Scheme
National Information Assurance Partnership
National Institute of Standards & Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930

DRAFT - for Review and Comments

Annex D. Sample Observation Report Format

Tracking ID:

Short Title:

Submission Date:

Decision Date:

Project Expiration Date: (Current estimated project completion date + 6 months)

CCTL:

CCTL Tracking ID:

CCTL POC:

Validator:

Evaluation: (The evaluation for which the OR is being submitted)

Evaluation Type: (PP) (TOE) (TOE against PP)

Evaluation Target: (Which PP or EAL for ST only)

Issue for which a resolution is requested:

Issue Type: (Scheme process or technical evaluation)

Proposed resolution to the issue and impact: (may include various resolutions and respective impacts)

Background for the decision process (should include validator comments):

References: (CC, CEM, CCEVS documents, etc., including document version and paragraph references)

Annex E. Validation Report Format

Validation Report and Its Use

The Evaluation Technical Report (ETR) is written by the CCTL for the Validation Body and serves as the principal basis for the Validation Report. The objective of the ETR is to present all verdicts, their justifications and any findings derived from the work performed during the evaluation, including errors found during the development of the information technology product or protection profile and any exploitable vulnerabilities discovered during the evaluation. The ETR may contain protected information as necessary to justify evaluation results.

The Validation Report is the source of detailed security information about the information technology product or protection profile for any interested parties. Its objective is to provide practical information about the product or protection profile to consumers. The Validation Report need not, nor should contain protected information since, like the Security Target, it contains information for the consumer necessary to securely deploy the evaluated product.

Executive Summary

The executive summary is a brief summary of the entire report. The information contained within this section should provide the audience with a clear and concise overview of the evaluation results. The audience for this section could include developers, consumers and evaluators of secure information technology systems and products. It may be that the reader will be able to gain a basic familiarity with the product or the protection profile and the report results through the executive summary. Some clients, (e.g., accreditors, management) may only read this section of the report, therefore, it is important that key evaluation findings be included in this section. An executive summary should contain, but is not limited to the following items:

- a) Name of the evaluated IT product, enumeration of the components of the product that are part of the evaluation, developer's name, and version;
- b) Name of CCEVS CCTL;
- c) Completion date of evaluation; and
- d) Brief description of the report results:
 - 1) assurance package;
 - 2) functionality;
 - 3) summary of threats and Organizational Security Policies (OSPs) addressed by the evaluated IT product;
 - 4) special configuration requirements
 - 5) assumptions about the operating environment
 - 6) disclaimers

DRAFT - for Review and Comments

B.2 Identification

The evaluated IT product has to be clearly identified. The software version number, any applicable software patches, hardware version number, and peripheral devices (e.g., tape drives, printers, etc.) must be identified and recorded. This provides the labeling and descriptive information necessary to completely identify the evaluated IT product. Complete identification of the evaluated IT product will ensure that a whole and accurate representation of the IT product can be recreated for use or for future evaluation efforts.

B.3 Security Policy

The security policy section should contain the description of the IT product's security policy. The security policy describes the IT product as a collection of security services. The security policy description contains the policies or rules that the evaluated IT product must comply with and/or enforce.

B.4 Assumptions and Clarification of Scope

The security aspects of the environment/configuration in which the IT product is expected to be used in should be included in this section. The section provides a means to articulate the clarification of the scope of the evaluation with respect to threats that are not countered. Users can make informed decisions about the risks associated with using the IT product. Usage, environmental assumptions, and clarification of the scope of the evaluation with respect to threats that are not countered should be stated in this section.

B.4.1 Usage Assumptions

In order to provide a baseline for the product during the evaluation effort, there are certain assumptions about the usage of the IT product that must be made. Items such as proper installation and configuration, minimum hardware requirements being satisfied, etc., all have to be assumed. This section documents any usage assumptions made about the IT product during the evaluation.

B.4.2 Environmental Assumptions

In order to provide a baseline for the IT product during the evaluation effort certain assumptions about the environment the product is to be used in has to be made. This section documents any environmental assumptions made about the IT product during the evaluation.

B.4.3 Clarification of Scope

DRAFT - for Review and Comments

This section lists and describes threats to the IT product that are not countered by the evaluated security functions of the product. Some clients may assume that the product counters threats when this is not the case. Therefore these threats that are not countered by the product should be listed for clarification. It would however, be impractical to list all possible threats that cannot be countered by an individual product.

B.5 Architectural Information

This section provides a high level description of the IT product and its major components based on the deliverables described in the Common Criteria assurance family entitled Development-High Level Design (ADV_HLD). The intent of the section is to characterize the degree of architectural separation of the major components.

B.6 Documentation

A complete listing of the IT product documentation provided with the product by the developer to the consumer is listed in this section. It is important that all relevant documentation be noted with the version numbers. The documentation at a minimum describes the user, administration and installation guides. It may occur that the administration and installation guide information is contained in a single document.

B.7 IT Product Testing

This section describes both the developer and the evaluator testing effort, outlining the testing approach, configuration, depth, and results.

B.8 Evaluated Configuration

This section documents the configuration of the IT product during the evaluation. Typically, the administrator or installation guide will provide the necessary details for the correct configuration of the IT product. The IT product may be configurable in a number of different ways depending on the environment it is used in or the security policies of the organization that it enforces.

The precise settings and configuration details with accompanying rationale for these choices are outlined in this section. Any additional operational notes and observations can also be included. This section is of particular importance, as it provides a baseline for the evaluated product installation.

B.9 Results of the Evaluation

DRAFT - for Review and Comments

This section documents the assurance requirements that the IT product satisfies. A detailed description of these requirements, as well as the details of how the product meets each of them can be found in the Security Target.

B.10 Evaluator Comments/Recommendations

This section is used to impart additional information about the evaluation results. These comments/recommendations can take the form of shortcomings of the IT product discovered during the evaluation or can mention features that are particularly useful.

B.11 Annexes

The Annexes are used to outline any additional information that may be useful to the audience of the report but does not logically fit within the prescribed headings of the report (e.g., complete description of security policy).

B.12 Security Target

The Security Target must be included with the Validation Report.

B.13 Glossary

The Glossary is used to increase the readability of the report by providing definitions of acronyms or terms of which the meaning may not be readily apparent.

B.14 Bibliography

The Bibliography section lists all referenced documentation used as source material in the compilation of the report. This information can include but is not limited to:

- criteria, methodology, program scheme documentation;
- technical reference documentation; and
- developer documentation used in the evaluation effort.

Annex F. CCEVS Evaluation Workplan Template

The objective of an Evaluation Workplan is to define and justify the work packages to be performed in order to satisfy the objectives of the evaluation.

Evaluation Workplan Contents

Chapter 1 - Introduction

This chapter of the workplan contains an introduction to the plan (not to the evaluation), and should comprise the following sections:

Background - should include the following information:

- a. the name of the product to be evaluated
- b. the identity of the Developer
- c. the identity of the Sponsor (if different from the developer)
- d. reference to the Security Target of the TOE

Scope – state whether this workplan covers all of the planned activities associated with the evaluation, and if not, how the plan will be updated.

Structure – describe the structure of the document for the reader.

Chapter 2 - Description of the TOE

This chapter of the workplan should provide a description of the TOE to be evaluated in sufficient detail to enable the rest of the document to be understood.

1. **TOE Overview** – should provide a description of the TOE, the functions it is to perform
2. **TOE Architecture** – should summarize the top-level design of the TOE and any constraints on this design
3. **TOE Documentation** - should describe the major documents produced by the Developer or Sponsor, together with their inter-relationships.

Chapter 3 - Evaluation Jobs

The work to be performed preformed during an evaluation is preformed as one or more evaluation jobs, each comprising a set of work packages. This chapter should contain a section providing a description of each of the proposed evaluation jobs, including:

DRAFT - for Review and Comments

- Objective
- Scope
- Associated Work packages (including a brief description)
- Expected Start and end dates of each evaluation job
- Milestones associated with each evaluation job (e.g., projected dates of penetration tests, issue of the ETR to the CCEVS)

For each work package, the emphasis is on a brief description since a detailed specification for each work package should be contained in Annex A of the workplan.

Chapter 4 - Workplan Rationale

It is important to demonstrate that the work proposed is appropriate. This is necessary to ensure that the correct work is preformed and also that neither too much, nor too little, work is preformed. This is achieved by giving a rationale for the work. This rationale will comprise the following:

- An explanation of how the work is consistent with the Scheme
- An explanation of how the work is consistent with the Evaluation methodology as described in the Common Methodology
- An explanation of how the work is consistent with the target evaluation level(s) (i.e., all the relevant CC evaluator actions have been addressed and with an appropriate degree of rigor).

Chapter 5 - Constraints

This chapter should contain any factors that the evaluators consider will constrain the work planned for the evaluation, and discuss the consequences of the constraints for the evaluation. The constraints will vary from evaluation to evaluation, but possible examples include:

- Evaluation resources
- Development schedules
- Timing and duration of access to the operational TOE may be limited
- Deadlines for the completion of the evaluation
- Contact with one or more organizations involved with the evaluation may be limited (or even prohibited)
- Requirements for the evaluators to use specific tools or techniques.

Annex A – Work Package Specifications

This annex should contain a detailed specification of each work package described in the workplan. The objective of each specification is to define the work to be performed, in sufficient detail for:

DRAFT - for Review and Comments

- An evaluator to undertake the work , knowing what is required
- The CCEVS and evaluators to be satisfied that the proposed work is necessary and, together with the work proposed in the other work package specifications, sufficient to satisfy the requirements of the evaluation.

Each work package specification should be comprised of the following sections:

1. Objective: stating the objectives of the work defined in the work package specification
2. Required Inputs: stating the evaluation deliverables that will be required to perform the work (e.g., design documentation, access to the implemented TOE)
3. Techniques and Tools: stating how the work is to be performed and identifying specific tools and techniques that will be used to achieve the work package objectives

Annex B – Outline Evaluation Plan

This annex should contain a bar chart or Gantt chart depicting the planned start and end dates of each proposed evaluation job and work package.

Annex C – Schedules and Resources

This annex should contain details of the schedules and resources for each work package. This information may be regarded by the CCTL as being proprietary and is therefore included in a separate annex to enable this information to be separated from the document if it is to be circulated outside of the CCTL or CCEVS. The information presented for each work package should include:

- The total amount of effort required to perform the work
- The number of evaluators required to perform the work
- Planned start and end dates.

DRAFT - for Review and Comments

Annex G. Evaluation Acceptance Agreement

EVALUATION ACCEPTANCE AND NON-DISCLOSURE AGREEMENT

THIS AGREEMENT, made this _____ day of _____, 19____, is between _____, hereinafter referred to as Sponsor, _____, hereinafter referred to as CCTL, and the National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme, hereinafter referred to as CCEVS.

WHEREAS, the Sponsor, CCTL, and CCEVS desire to enter into evaluation and discussions concerning a product described as _____ submitted to CCEVS. To enable the CCEVS to conduct the necessary government oversight of the evaluation of the product by the CCTL, it may be necessary for the CCTL and/or Sponsor to disclose to the CCEVS certain information which is proprietary to the Sponsor and/or CCTL ("Proprietary Information").

NOW THEREFORE, to protect such Proprietary Information the Sponsor, CCTL, and CCEVS agree as follows:

1. Proprietary Information may include, without limitation, trade secrets, business plans, financial data, technical data, and other items pertaining to the above proposed product as be necessary or desirable to conduct the evaluation.

2. To be protected hereunder, all Proprietary Information provided to the CCEVS must be clearly identified and properly marked by the Sponsor and/or CCTL so that such information can be protected by the CCEVS to the full extent authorized by law.

3. To the extent permitted by law all Proprietary Information provided under this agreement will be held in strict confidence and only used as necessary to perform the evaluation and evaluation oversight. If required, the CCEVS will actively solicit the Sponsor's and CCTL's assistance in establishing supportable bases for protecting such Proprietary Information in response to Freedom of Information Act requests. CCEVS will not transfer or assign any Proprietary Information outside of CCEVS without prior written consent of the Sponsor and/or CCTL as appropriate.

4. No grant, ownership, license, or right other than as specified herein is transferred hereby. No modification of any kind of the Source Code or any other Proprietary Information is permitted under this Agreement without the prior written permission of the Sponsor. Specifically, CCEVS agrees not to alter, remove, or otherwise disturb any notices of intellectual or proprietary rights, including without limitation copyright. The Sponsor and/or CCTL are specifically not responsible for use of any Sponsor or CCTL Proprietary Information for other than an evaluation. Except as necessary to conduct an evaluation, reverse

DRAFT - for Review and Comments

engineering, decompilation and other source code derivations of any object code is specifically prohibited.

5. CCEVS shall not be liable for any unauthorized disclosure or use of Proprietary Information if it:

- (a) is presently known or hereafter becomes known to the public by other than breach of the CCEVS' obligations here under, or
- (b) is known to the CCEVS without restriction prior to the time disclosure of it by the Sponsor or CCTL, or
- (c) is subsequently and independently developed by the CCEVS without resort to the Sponsor's or CCTL's disclosure, or
- (d) is independently and rightfully acquired by the CCEVS from another source without restriction on disclosure or use, or
- (e) is identified by the Sponsor or CCTL to be no longer subject to this Agreement.

6. The receipt of this information by the CCEVS for the purpose of performing government oversight of the evaluation shall not be construed in any way as a commitment to the Sponsor or CCTL for any future procurement of any equipment or other items of supply or service sold by the Sponsor or CCTL nor in any way be permitted to provide a basis or argument for sole source procurement that might otherwise prevent free and full competition.

7. It is mutually understood and agreed that the evaluation oversight will be conducted by validators for the CCEVS. It is further understood and agreed that the CCEVS' validators may include authorized agents who are under contract with the CCEVS and who are bound to abide by all terms, conditions, and references of this Agreement.

8. Any report or other information provided by the CCEVS to the Sponsor and/or CCTL arising out of or as a result of this Agreement or the evaluation is not to be construed as an endorsement of the Sponsor's or CCTL's goods and/or services and the Sponsor and/or CCTL will not, by advertising or otherwise, claim or imply the existence of a CCEVS endorsement of its goods and/or services covered by this Agreement.

9. This Agreement shall be governed by, and construed in accordance with, federal statutes and regulations, notwithstanding any State conflict of law statutes, practices or rules of construction.

10. This Agreement is effective for a period of five years from the date that first appears in this Agreement. The CCEVS' obligation to protect Proprietary Information shall continue for a period of five (5) years following disclosure of such information to the CCEVS. Within ten (10) days of termination of this Agreement, CCEVS shall return all originals of the Source Code and any other Proprietary Information of the Sponsor or CCTL which has been fixed in any

DRAFT - for Review and Comments

tangible means of expression, and any copies thereof. It is further understood and agreed that for security reasons CCEVS will not return to the Sponsor or CCTL any software or magnetic media which has been installed on a CCEVS system and the CCEVS will destroy said software upon completion of the Agreement. Any documentation provided with the software will be returned to the Sponsor or CCTL upon termination as appropriate.

11. Neither failure to require performance, nor waiver of a breach, of any provision of this Agreement constitutes any waiver of a party's right to subsequently require full performance of that provision.

12. No promise of payment is made herein and this agreement constitutes the total obligation of the parties. This Agreement is the complete and exclusive statement of the parties on these specific subjects, and supersedes all prior written or oral agreements, proposals and understandings relating thereto.

13. This Agreement may only be modified in writing when signed by an officer of the party to be bound. If any court of competent jurisdiction determines that any provision of this Agreement is invalid, the remainder of the Agreement will continue in full force and effect, and the invalid provision shall be restated to most nearly give effect to its stated intent.

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme
100 Diamond Road
Gaithersburg, MD

BY: _____

TITLE _____

DATE: _____

SPONSOR'S NAME
Address
City, State

CCTL's NAME
Address
City, State

BY: _____

BY:

TITLE _____

TITLE

DATE: _____

DATE:

DRAFT - for Review and Comments

DRAFT - for Review and Comments

Annex H. Sponsor's Approval to List Products that are in Evaluation

This form authorizes the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) to post information contained herein about a product that is in process of being evaluated under NIAP CCEVS procedures.

The NIAP CCEVS maintains a "Validated Products List" and a separate list of products that are "In Evaluation". Both lists are publicly available and can be found on the NIAP CCEVS website, <http://niap.nist.gov/cc-scheme>. Validated products are those security-enhanced products that have been evaluated and have received a NIAP "Common Criteria Certificate". Products "in evaluation" are those security-enhanced products that are in the process of being evaluated by a NIAP CCEVS Common Criteria Testing Laboratory (CCTL) under CCEVS validation procedures.

If the sponsor/company DOES NOT wish to have information about a product "in evaluation" listed on the NIAP CCEVS website, then the sponsor must complete the "Name of Product" and "Sponsor/Company" section, check the DO NOT LIST block at the bottom of this form, sign the form and submit it to the CCEVS. The remaining information sections should be left blank.

If the sponsor/company wishes to have information about the product "in evaluation" listed on the NIAP CCEVS public website then the sponsor must complete all sections of this form, check the PLEASE LIST block, sign the form and submit the completed form to the CCEVS.

Name and Version of Product:

Product Type:

Assurance Level:

CCTL:

Sponsor/Company Name:

Sponsor Point of Contact:

Phone: _____

Email: _____

DRAFT - for Review and Comments

DO NOT LIST information on NIAP CCEVS website

PLEASE LIST information on NIAP CCEVS website

Print Name & Title:

(Name of authorized sponsor/company representative and title)

Signature or Email:

DRAFT - for Review and Comments

Annex I. Sample Kick-off Meeting Agenda

Sample Evaluation Acceptance Meeting Agenda

1. Validator:

- a. Identify purpose of the meeting,
- b. introduce participants and,
- c. review/adjust meeting agenda

2. Director/Deputy Director:

- a. Identify validation team members and their role in the evaluation process -- POC, quality & consistency, etc.;
- b. Identify scheme management POC and their role in the evaluation process -- monitor validator performance, source of appeal/complaint, etc.;
- c. Provide brief overview of NIAP NIST/NSA)/Scheme organization and goals;
- d. Provide brief overview of key participants and their roles (or scheme expectations) in the Scheme - NVLAP, Labs, sponsor & CCRA; and
- e. Provide brief statement of Scheme goals -- timely response to sponsor & lab questions, minimize impact of sponsor & lab schedules, handling of proprietary information, etc.

3. Sponsor:

- a. Identify Key POCs for project
- b. Give brief overview of product / PP
- c. Define goals, expectations and desired completion schedule of project

4. Lab:

- a. Identify Key POCs for project
- b. Give brief overview of evaluation plans
- c. Give brief overview of goals, expectations and issues

5. Validator:

- a. Provide brief overview of Validation Plan
- b. Provide brief overview of goals, expectations and issues
- c. Review of next scheduled activity/meeting

6. Open floor for Questions

7. Meeting Wrap-up

- a. Director/Deputy Director: Provide statement of acceptance (or non-acceptance) of project into the scheme, other administrative reminders, etc.
- b. Validator: Closing remarks, meeting summary, review of key points/schedules, etc.

DRAFT - for Review and Comments

Annex J. Common Criteria Certification Mark Policy

The Validation Body will monitor the use of CC certificates for each CCEVS validated product to verify that all rules associated with the use of the certificates are being adhered to.

Vendors may use the Common Criteria Certification Mark in conjunction with advertising, marketing, and sales of their Common Criteria validated product. "Validated 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 the NIAP CCEVS and are listed on the NIAP Validated Products List (VPL).

Potential uses for the Certification Mark

Products & Packaging

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

Brochures

Vendors may use the Certification Mark in marketing/sale brochures. If the Certification Mark appears at the top of a one-page brochure, all text and graphics must refer ONLY to the validated product. If the Certification mark appears at the top of a page within a multi-page brochure, all text and graphics that appear on the same page as the logo must refer ONLY to the validated product. The specific version number, as listed on the Validated Products 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 validated product. The version number, as listed on the VPL, must be included.

Signs, Trade Show Backdrops, etc.

Only the validated 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 validated product. The validated product name and version number, as listed on the VPL, must be included on the sign, banner, backdrop, etc., so that it is clear that the logo refers to the validated product.

Scheme Point of Contact

For general information about the Certification Mark use, vendors should contact Mrs. Rebecca Galanakis in the NIAP Common Criteria Evaluation and Validation Scheme on 410-854-4458. Prior to initial use of the Certification Mark, vendors must provide the scheme point of contact copies of the intended use of 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 will result in revocation.

DRAFT - for Review and Comments

Annex K. Evaluation Technical Report Outline for a Target of Evaluation

DRAFT - for Review and Comments

Evaluation Technical Report for a Target of Evaluation

[Name of the TOE, date (if applicable) and version number goes here (include patches number and other applicable version numbers that uniquely identify the TOE)]

[List the version number and date of the Security Target (ST) here]
[List the PP(s) that the TOE is claiming compliance to here (List the name(s), version numbers and dates of the PP(s)).]

[Version number of ETR goes here along with the date of the report]

Evaluated by:

[Name of the evaluation facility with laboratory logo]

Prepared for:

**National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme**

DRAFT - for Review and Comments

The Developer of the TOE:

[The developer of the TOE goes here (name, address...)]

The TOE Evaluation was sponsored by:

[The sponsor of the TOE evaluation goes here (name, address...)]

Evaluation Personnel:

[List of evaluation personnel]

DRAFT - for Review and Comments

Common Criteria Version

[Version number and date goes here]

Common Evaluation Methodology Version

[Version number and date goes here]

National Interpretations

[List the National Interpretations that affected the evaluation here. The number of the interpretation followed by the title of the interpretation should be listed. One listing per line.

[Interpretation # and title go here]

International Interpretations

[List the International Interpretations that affected the evaluation here. The number of the interpretation followed by the title of the interpretation should be listed. One listing per line.

[CCIMB-INTERP # and title go here]

DRAFT - for Review and Comments

1. TOE Overview

[This section of the ETR should present a high-level overview of the TOE. It should briefly describe the TOE. The purpose of this overview is to provide an introduction to specific concepts that might be necessary to understand subsequent sections of the report, as well as to provide a picture of what is under evaluation.]

For this section it may be appropriate to reference sections of the ST.]

2. Architectural Description of the TOE

[This section provides a high level description of the IT product and its major components based on the deliverables described in the Common Criteria assurance family entitled Development High Level Design (ADV_HLD). The intent of the section is to characterize the degree of architectural separation of the major components. This section is not going to be needed if the assurance family ADV_HLD is not present in the assurance package of the Security Target.]

3. Evaluation

[In this section the evaluator reports the evaluation methods, techniques, tools and standards used. The evaluator may reference the devices used to perform the tests.]

The evaluator reports any constraints on the evaluation; constraints on the distribution of evaluation results and assumptions made during the evaluation that have an impact on the evaluation results. The evaluator may include information in relation to legal or statutory aspects, organization, confidentiality, etc.]

4. Results of Evaluation

[This section of the ETR presents the results of the evaluation. Assurance results of the evaluation are reported in this section of the ETR.]

Interpretations (National and International) are to be considered for all evaluation results that are reported in the ETR.]

4.1 Assurance Requirement Results

[This section reports assurance requirement results.]

4.1.1 Common Criteria Assurance Components

[The evaluator is to report all information specifically required by a CEM work unit.]

For each activity on which the ST and product/system is evaluated, the evaluator shall report:

- the title of the activity considered;
- a verdict and a supporting rationale for each assurance component that constitutes this activity, as a result of performing the corresponding CEM action and its constituent work units.

The rationale justifies the verdict using the CC, the CEM, any interpretations and the evaluation evidence examined and shows how the evaluation evidence does or does not meet each aspect of the criteria. It contains a description of the work performed, the method used, and any derivation of results. The rationale may provide detail to the level of a CEM work unit.]

4.1.1.1 Testing and Vulnerability Assessment

[The testing and vulnerability assessment activities conducted during the evaluation are to be reported by the evaluator in the ETR. The reporting and level of detail is to be based on the testing and vulnerability components that appear in the ST.]

For the AVA and ATE activities, work units that identify information to be reported in the ETR have been defined.]

DRAFT - for Review and Comments

4.1.2 Assurance Components without Methodology

[There are potentially three circumstances that exist when an assurance activity will not have methodology written for it. These circumstances are:

- Common Criteria assurance components that do not contain methodology in the CEM,
- Explicitly stated assurance activities, and
- National and International Interpretations that affect a Common Criteria assurance requirement in a way that requires new methodology to satisfy the interpretation.

If any of these circumstances affect the evaluation proper reporting of the developed methodology and results of applying the developed methodology need to be undertaken in the ETR. The methodology developed needs to be included and reported to the level of detail that is specified in the other assurance sections of the ETR.

When testing and vulnerability assessment assurance methodology needs to be developed the CCTL needs to work with CCEVS to specify what needs to be reported with in the ETR. In general, testing and vulnerability assessment documents generated by the CCTL and the activities carried out by the CCTL to satisfy the methodology will need to be reported in the ETR.]

4.1.3 Supplemental Security Functional Requirement Results - OPTIONAL

[The evaluation team is not required to include this section in the report. At the team's discretion, this section of the report would contain supplemental material describing the TOE's satisfaction of the security functional requirements, if such material is deemed helpful. Information presented in this section is that which has not already been included in the contents of the TSS.]

5. Conclusions

[The evaluator shall report the conclusions of the evaluation, which will relate to whether the TOE has satisfied its associated ST, in particular the overall verdict as defined in CC Part 1 Chapter 5, and determined by application of the verdict assignment described in Section 1.4, Evaluator verdicts.

Any conclusion statements should be constrained to the functional and assurance requirements, environment, and objectives specified in the ST.]

6. Recommendations

[The evaluator provides recommendations that may be useful for the CCEVS and the Validator. These recommendations may include shortcomings of the IT product discovered during the evaluation or mention of features that are particularly useful.

Any recommendation statements should be constrained to the functional and assurance requirements, environment, and objectives specified in the ST.]

7. Evaluation Evidence

[The evaluator shall report for each item of evaluation evidence the following information:

- the issuing body (e.g. the developer, the sponsor);
- the title;
- the unique reference (e.g. issue date and version number).]

8. Validated Products List (VPL) Entry

[This section should contain the VPL entry for the TOE that will be posted on the web-site.]

9. List of Acronyms

[The evaluator reports any acronyms or abbreviations used in the ETR.]

DRAFT - for Review and Comments

10. Glossary of Terms

[Glossary definitions already defined by the CC or CEM need not be repeated in the ETR. The evaluator needs only report those that are specific to this evaluation.]

11. Observation Reports and Decisions

[The evaluator includes a listing of all observation and decisions reports submitted and received during the course of the evaluation.]

12. National and International Interpretations

[The evaluator includes in full a description of all National and International Interpretations that effected the evaluation. The ETR reports the interpretations as posted by the Scheme and the International CC Community.]

13. Security Target

[The Security Target is considered part of the ETR. It is submitted with the ETR as a separate document.]

DRAFT - for Review and Comments

Annex L. Evaluation Technical Report Outline for a Protection Profile

*Evaluation Technical Report
For a
Protection Profile*

[Name of Protection Profile, date and version number goes here]

[Version number of ETR goes here along with the date of the report]

Evaluated by:

[Name of the evaluation facility with laboratory logo]

Prepared for:

**National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme**

DRAFT - for Review and Comments

Protection Profile was developed by:

[The developer of the Protection Profile goes here (name, address...)]

The Protection Profile Evaluation was sponsored by:

[The sponsor of the Protection Profile goes here (name, address...)]

Evaluation Personnel:

[List of evaluation personnel]

DRAFT - for Review and Comments

Common Criteria Version

[Version number and date goes here]

Common Evaluation Methodology Version

[Version number and date goes here]

National Interpretations

[List the National Interpretations that affected the evaluation here. The number of the interpretation followed by the title of the interpretation should be listed. One listing per line.]

[Interpretation # and title goes here]

International Interpretations

[List the International Interpretations that affected the evaluation here. The number of the interpretation followed by the title of the interpretation should be listed. One listing per line.]

[CCIMB-INTERP # and title goes here]

DRAFT - for Review and Comments

1. PP Overview

This section of the ETR should give an overview of the PP (the IT technology that it is modeling).

For this section it may be appropriate to reference sections of the PP.

2. Evaluation

In this section the evaluator reports the evaluation methods, techniques, tools and standards used. The evaluator references the evaluation criteria and methodology.

The evaluator reports any constraints on the evaluation, constraints on the handling of evaluation results, and assumptions made during the evaluation that have an impact on the evaluation results. The evaluator may include information in relation to legal or statutory aspects, organization, confidentiality, etc.

3. Results of the evaluation

The evaluator shall report a verdict and a supporting rationale for each assurance component that constitutes an APE activity, as a result of performing the corresponding CEM action and its constituent work units.

The rationale justifies the verdict using the CC, the CEM, any interpretations and the evaluation evidence examined and shows how the evaluation evidence does or does not meet each aspect of the criteria. It contains a description of the work performed, the method used, and any derivation of results. The rationale may provide detail to the level of a CEM work unit.

3.1 Assurance Components without Methodology

There are potentially three circumstances that exist when an assurance activity will not have methodology written for it. These circumstances are:

- Common Criteria assurance components that do not contain methodology in the CEM,
- Explicitly stated assurance activities, and
- National and International Interpretations that affect a Common Criteria assurance requirement in a way that requires new methodology to satisfy the interpretation.

If any of these circumstances affect the evaluation proper reporting of the developed methodology and results of applying the developed methodology need to be undertaken in the ETR. The methodology developed needs to be included and reported to the level of detail that is specified in the other assurance sections of the ETR.

4. Conclusions

The evaluator shall report the conclusions of the evaluation, in particular the overall verdict as defined in CC Part 1 Chapter 5, and determined by application of the verdict assignment described in Section 1.4, Evaluator verdicts.

5. Recommendations

The evaluator provides recommendations that may be useful for the Validation Body. These recommendations may include shortcomings of the PP discovered during the evaluation or mention of features that are particularly useful.

6. Evaluation evidence

The evaluator shall report for each item of evaluation evidence the following information:

- the issuing body (e.g. the developer, the sponsor);
- the title;
- the unique reference (e.g. issue date and version number).

7. Validated Products List (VPL) Entry

DRAFT - for Review and Comments

[This section should contain the VPL entry for the PP that will be posted on the web-site.]

8. List of acronyms

The evaluator shall report any acronyms or abbreviations used in the ETR.

9. Glossary of terms

Glossary definitions already defined by the CC or CEM need not be repeated in the ETR.

10. Observation reports and decisions

The evaluator includes all observation reports and decisions submitted and received during the course of the evaluation. The ETR needs to make clear in this section which observation decisions is being used to satisfy which observation report.

11. National and International Interpretations

The evaluator includes all National and International Interpretations that affected the evaluation. The ETR reports the interpretations as posted by the Scheme and the International CC Community.

12. Protection Profile

[The Protection Profile is considered part of the ETR. It is submitted with the ETR as a separate document.]