



Common Criteria Evaluation and Validation Scheme

Publication #4

Guidance to CCEVS Approved Common Criteria Testing Laboratories

8 September 2008
Version 2.0

Foreword

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

Audrey M. Dale
Director, CCEVS

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

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

Amendment record

Version	Date	Description
Draft 1.0	20 March 2001	Initial release.
2.0	8 September 2008	Complete revision based on current operations

(This page intentionally left blank)

Table of Contents

1	Introduction.....	1
1.1	Purpose	1
1.2	Organization and Scope.....	1
2	Common Criteria Testing Laboratory	2
2.1	Requirements for CCTL Approval	2
2.1.1	CCEVS-Specific Requirements	3
2.1.2	NVLAP Accreditation	4
2.2	Extending CCTL Scope of Accreditation.....	4
2.3	Renewal of Approval/Accreditation	4
2.4	Withdrawal or Suspension of Approval/Accreditation.....	5
2.5	Audits.....	5
2.6	Notifying CCEVS of CCTL operation changes	5
2.7	Independence and Conflict of Interest.....	6
2.7.1	CCEVS Conflict of Interest Guidelines.....	6
2.8	Proprietary/Sensitive Information	7
2.9	Evaluation of Assurance Levels (EALs) 5 through 7	7
3	Preparation for IT Security Evaluation	7
3.1	Letter of Interest (LOI) Requirement	8
3.2	Acceptance of Security Targets (STs).....	8
3.3	Acceptable TOEs for Evaluation.....	8
3.4	STs Claiming Conformance to a Validated PP.....	8
4	Validation Process	9
4.1	Validation Oversight Review (VOR) Process	9
4.2	Technical Oversight Panel (TOP).....	9
4.3	Observation Reports and Decisions.....	10
5	Government Roles in Evaluation and Validation	10
5.1	Government Evaluators	10
5.2	Government Validators.....	11
5.3	Record Keeping	11
5.4	Time Limits on CCEVS Evaluations.....	12
6	Concluding an evaluation/validation	12
	Annex A: References.....	14
	Annex B: Acronyms.....	15
	Annex C: Glossary	17
	Annex D: Letter of Intent.....	20
	Annex E: Sample CCTL & CCEVS Non-Disclosure Agreement.....	21

1 Introduction

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

The principal participants in the CCEVS program are the:

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

1.1 Purpose

The purpose of this document is to describe the process for becoming an approved CCTL and to help the CCTL personnel prepare for and understand their role prior to, during, and after an IT product/system or PP evaluation.

1.2 Organization and Scope

This document is one of a series of technical and administrative CCEVS publications that describes how the scheme operates. It consists of seven chapters and several supporting annexes. Chapter 1 provides a high level overview of CCEVS. Chapter 2 provides requirements for candidate and approved CCTLs, Chapter 3 provides details on the CCTLs role in preparing for an evaluation, Chapter 4 provides an overview of the validation process, Chapter 5 discusses the Government roles associated with evaluations, and Chapter 6 provides information on concluding the evaluation/validation.

The supporting annexes cover a variety of topics to include a sample Letter of Intent and CCTL & CCEVS Non-Disclosure Agreement as well as a glossary and list of commonly used acronyms.

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

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

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

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

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

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

CCEVS related publications and information are available through the [CCEVS web site](#).

2 Common Criteria Testing Laboratory

Organizations interested in becoming a CCTL must go through a series of steps that involve both the CCEVS and NVLAP. Rather than develop its own accreditation capabilities, the CCEVS has delegated the responsibility of CCTL accreditation to NVLAP. Accreditation by NVLAP is the primary requirement for achieving CCTL status. The CCEVS worked closely with NVLAP to establish CC specific requirements to ensure the laboratory demonstrates appropriate CC/technical knowledge and understanding as part of their accreditation. A testing laboratory becomes a CCTL when they are accredited by NVLAP and approved by the CCEVS and is listed on the CCEVS Approved CCTL List.

The CCEVS has responsibility for the oversight of evaluations performed by CCTLs. In addition to technical oversight (validation) of every evaluation, CCEVS grants approval for a candidate CCTL to become an approved CCTL, modifies approval, and coordinates with NVLAP to conduct audits. The actions for each of these are addressed below.

2.1 Requirements for CCTL Approval

The CCEVS grants approval for candidate CCTLs to become a CCEVS CCTL when all CCEVS-specific and NVLAP accreditation requirements have been successfully met.

Once all requirements have been met, the candidate CCTL is approved by the CCEVS to conduct IT security evaluations up to and including the approved EAL of its initial NVLAP accreditation and is placed on the CCEVS CCTL List.

2.1.1 CCEVS-Specific Requirements

The CCEVS imposes four CCEVS-specific requirements¹:

- a) CCTL must reside within the U.S. and be a non-governmental legal entity, be duly organized and incorporated and in good standing under the laws of the state where the CCTL intends to do business;²
- b) CCTL must agree to accept CCEVS technical oversight and validation of evaluation-related activities in accordance with the policies and procedures established by the scheme;
- c) CCTL must agree to accept U.S. Government participants in CCEVS-selected CC evaluations conducted by the CCTL in accordance with the policies and procedures established by the CCEVS;
- d) CCTL must be a third party independent evaluation facility; and
- e) CCTL must demonstrate technical and CC competencies as outlined in NIST Handbook 150-20, *Information Technology Security Testing—Common Criteria*

The CCEVS will:

1. verify the satisfaction of these requirements by confirming the content of the submitted "Letter of Intent," submitted by a candidate CCTL (For a sample Letter of Intent, see [Annex D](#).);

¹ The CCEVS 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.

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 CCEVS 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.

2. confirm and notify the CCTL of acceptance as a CCEVS Approved CCTL when all CCEVS-Specific requirements, and all NVLAP accreditation requirements have been met; and
3. document an agreement with the CCEVS Approved CCTL ([Annex E](#)).

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:

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 CCTL Scope of Accreditation

A NVLAP scope of accreditation is defined to be the specific *EAL* the CCTL has been accredited to use in conducting IT security evaluations. A candidate CCTL will choose the *EAL* it wishes to become accredited for from the CCEVS Approved *EAL*s.

CCTLs wishing to expand their scope of accreditation, 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 by the CCEVS. For the specific requirements

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.

for CCTLs during reaccreditation, see Handbook 150-20 Annex B– Reaccreditation Activities.

2.4 Withdrawal or Suspension of Approval/Accreditation

When the CCEVS 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 CCEVS 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 CCEVS Approved CCTL will be withdrawn.

The conditions for withdrawal and suspension of *CCEVS initial accreditation and reaccreditation* are described in the Annexes for Initial Evaluation Activities Handbook 150-20 (Annex A) and Reaccreditation Activities Handbook 150-20 (Annex B).

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

2.5 Audits

NVLAP or the CCEVS may audit a CCTL to ensure that the CCEVS requirements continue to be met. NVLAP will follow NIST Handbook 150 for its audit procedures. Auditing by either NVLAP or the CCEVS will be coordinated between them so 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 CCEVS and NVLAP upon request. CCTLs are also required to inform the CCEVS in writing of any changes in status that may cause a violation of a CCEVS requirement (e.g., change in ownership) or an NVLAP accreditation requirement.

2.6 Notifying CCEVS of CCTL operation changes

A CCTL must notify CCEVS management in writing if there are any significant changes in CCTL operations as described in the Letter of Intent or as the basis for NVLAP accreditation. Examples of events that require written notification are a CCTL's intent to withdraw from the CCEVS, 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 CCEVS if clarification is needed about whether a change is significant enough to warrant written notification.

2.7 Independence and Conflict of Interest

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 CCEVS. 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 CCEVS.

2.7.1 CCEVS Conflict of Interest Guidelines

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

Neither the CCTL, its parent corporation, nor any individual CCTL staff member concerned with a particular 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 CCEVS 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 CCEVS 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 CCEVS.

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. Details of the contract between the CCTL and the sponsor are for those two parties to negotiate, with no CCEVS involvement.

2.8 Proprietary/Sensitive Information

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

2.9 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 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.

Evaluations with components above EAL4 may require NSA involvement. The CCEVS will allow EAL4-accredited CCTLs to conduct evaluations with components above EAL4 that require NSA resources in accordance with [CCEVS Policy #19](#).

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 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). 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. Preparation for an IT evaluation includes a preliminary evaluation to ensure that the ST/PP meets the CCEVS minimum requirements for acceptance. These minimum requirements, explained below include; a Letter of Interest, acceptance of Security Targets (STs) into NIAP CCEVS evaluation, and Acceptable TOEs for Evaluation. Once the CCTL has confidence that the ST meets these minimum requirements, they should begin the ASE work units in preparation for submission to CCEVS.

3.1 Letter of Interest (LOI) Requirement

The CCTL must provide CCEVS with a detailed [Letter of Interest](#) (LOI) supplied by the Sponsor. CCEVS will not accept evaluations that do not have valid U.S. Government customers as outlined in CCEVS [Policy #12](#). The LOI is required prior to the scheduling of the Initial Validator Oversight Review (IVOR) and may be submitted along with the read-ahead submission or sooner, if available.

3.2 Acceptance of Security Targets (STs)

CCEVS [Policy #10](#) provides guidelines for acceptance of STs for evaluation. In particular, the Target of Evaluation (TOE) Description section and the Security Functional Requirements (SFRs) must be precisely written to accurately reflect the product and must provide the detailed information necessary to perform an evaluation. This policy should be referenced to ensure that the information provided in the ST meets CCEVS requirements.

3.3 Acceptable TOEs for Evaluation

A TOE considered acceptable for CCEVS evaluation must meet the requirements specified in [Policy #13](#). That policy defines requirements for the physical and logical boundaries of the TOE, PP compliance claims, and TOE functionality.

3.4 STs Claiming Conformance to a Validated PP

When the TOE Security Target claims conformance to a validated Protection Profile and there is a direct one for one mapping with the content of a successfully evaluated PP, the CCTL may claim conformance to the corresponding ASE requirements based on the protection profile APE evaluation evidence/analysis. This case requires no additional analysis of the ASE requirements.

If the TOE security target is a superset of the protection profile requirements, the sponsor and CCTL may claim partial conformance to the corresponding ASE requirements based

on the previous PP APE evaluation evidence/analysis. In general, exceeding the PP requirements has no effect on compliance; the ST writer may include more detail and additional capabilities that exceed the minimum requirements specified in the PP and remain compliant with the PP. However, this case requires that the ST author (and the corresponding TOE developer) demonstrate that the features and capabilities that are provided in addition to what is required in the PP neither introduce security vulnerabilities nor circumvent or interfere with required security functions.

The CCTL must complete the work units for the analysis of the TSS. Additionally, for each corresponding APE/ASE work unit, the CCTL must show that a review/mapping was conducted and provide a statement as to why the PP evaluation evidence/analysis is reusable between the PP and ST.

4 Validation Process

4.1 Validation Oversight Review (VOR) Process

Once the CCTL and Vendor have completed all preparation work described above, the evaluation and validation process begins. To achieve oversight activities, the CCEVS employs a Validation Oversight Review (VOR) process. The primary goal of the VOR process is for CCEVS to ensure the technical quality and consistency of the evaluation, to confirm that the CCTL correctly applied all CCEVS policies, and to verify the CCTL accomplished all required tasks (including analysis and testing). The VOR process is designed to provide oversight at specific milestones during each evaluation. Evaluations must successfully complete all validation activity associated with each milestone prior to proceeding to the next. The milestones identified by CCEVS include read-ahead submission, Initial VOR (IVOR), Kick-off, Test VOR (TVOR), Testing, Final VOR (FVOR) and Evaluation Conclusion/VPL Listing.

Detailed procedures describing the validator activities and the evaluator activities to demonstrate an understanding and successful analysis of the product under the CCEVS are described in the [*Validation and Oversight Review \(VOR\): Evaluations and Validators Guide*](#).

4.2 Technical Oversight Panel (TOP)

Although the VOR process is utilized for all evaluations, certain evaluations require additional oversight. CCEVS will utilize Technical Oversight Panels (TOPs) for higher assurance evaluations (EAL6 and EAL7), candidate laboratory evaluations, CCTL reaccreditations, or when CCEVS determines additional validator oversight is necessary. TOPs are similar to VORs but have a greater number of validators for additional oversight. For candidate laboratory evaluations, the TOP process is outlined in NIST Handbook 150-20:2005, Annex A. For CCTL reaccreditations, the TOP process is

outlined in NIST Handbook 150-20:2005, Annex B (revised 2008-01-07). Annex H of [Publication #3](#), describes the TOP process in detail.

4.3 Observation Reports and Decisions

An Observation Report 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 an issue, provides background information and offers a proposed solution. The CCTL submits the OR to the Validator for submission to CCEVS. CCEVS uses the OR to review the issue and develop clarification/guidance for the CCTL. The CCEVS formally responds to the CCTL by issuing an Observation Decision (OD) for each OR. The OR Process is described in detail in [Publication #3](#).

5 Government Roles in Evaluation and Validation

Government evaluators are assigned as members of a CCTL evaluation team at the sole discretion of CCEVS. If assigned, the CCTL will regularly interface with them and will include them in all evaluation team activities. The CCTL must also interact regularly with the government validators who are assigned to oversee every evaluation. This section describes the responsibilities of these two CCEVS representatives.

5.1 Government Evaluators

The government evaluator (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 an evaluation-related reason, and the lab cannot decline the assignment. 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 work plans, 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 evaluation team leader, taking into account the skills, interests, and abilities of the individual. The GE is expected to follow the lab's processes and procedures. The GE may 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 may not use GEs as a cost saving opportunity. The bids submitted by CCTLs to a potential evaluation sponsor must not depend upon the assignment of a GE to an evaluation team. Rather, the CCTLs must accept a GE if assigned by the government.

5.2 Government Validators

A validator is assigned to each evaluation to act as a liaison between the CCEVS 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 responsibilities of the validator are to provide guidance to the team on evaluation issues and to act on behalf of CCEVS to ensure the technical quality of the analysis performed. At the completion of the evaluation, the validator produces a Validation Report that provides an assessment of the evaluation process and the team's analysis.

At the discretion of CCEVS, validators may also observe testing. If it is decided that the validator will observe testing, the dates for testing must be determined and the validator must be notified of the date for testing. This date must be provided to the validator at least one month prior to the testing start date. In order to allow the validator to witness testing activities, all IVOR read-ahead submissions must include the planned testing location for the evaluation. In addition, if validators are required to observe testing, it must occur in the Continental United States (CONUS) or Canada in order to permit validation oversight. Exceptions to this location requirement may be granted on a case-by-case basis at the discretion of CCEVS, but will require a significant justification for exception.

5.3 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. For each evaluation, the CCTL must create an evaluation work plan for their quality system records. The work plan must include 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. These records will be utilized by the validator as part of the VOR process.

CCTL records are critical to the validator throughout the validation. The validator gains confidence in the CCTL's ability to define and correctly perform the required analysis for the evaluation by reviewing the evaluation records. 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, 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.

5.4 Time Limits on CCEVS Evaluations

An escalating complaint against the U.S. CC Scheme is the amount of time it takes to complete evaluations. Time limits bounding the duration of an evaluation have been established in order to address this complaint and to ensure proper use of limited CCEVS resources. Because product lifecycles continue to decrease, evaluation time limitations are also essential in ensuring the relevancy of evaluated products. Further details on evaluation time limits may be found in [CCEVS Policy # 18](#).

6 Concluding an evaluation/validation

The publication of the Validated Products List entry and the issuance of the certificate conclude an evaluation/validation.

Upon completion of the evaluation analyses, the CCTL will provide the Validator with the final ST, and Evaluation Technical Report (ETR), as defined by the CEM), all evaluation Observation Reports (ORs) along with any corresponding Observation Decisions (ODs), a draft Validated Products List entry and a draft Validation Report (VR). The ETR should be complete, including proprietary and/or sensitive information. The format and content requirements for the ETR are provided on the CCEVS website at the following URL: <http://www.niap-ccevs.org/cc-scheme/forms/>

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

The Director, CCEVS will make the decision to either:

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

The contents of a CC certificate are described in [Publication #1, Organization, Management and Concept of Operations](#). There are rules associated with the use of the

CCEVS certificate and the CC Certification Mark. See [Publication #5](#) for the CC Certification Mark Usage Policy.

Annex A: References

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

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

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

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

- Part 1 Introduction and general model
- Part 2 Security functional components
- Part 3 Security assurance components

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

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

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

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

Annex B: Acronyms

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

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

Annex C: Glossary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Annex D: Letter of Intent

This annex provides a sample letter of intent that may be used by prospective CCTLs to convey necessary administrative information to the CCEVS. This information will be used by the CCEVS to determine if the prospective CCTL has satisfied the scheme-specific requirements as articulated in this publication.

Company Letter Head		Date
Director Common Criteria Evaluation and Validation Scheme National Security Agency 9800 Savage Road Savage MD 20755-6757		
<p>This letter is formal notice that COMPANY NAME desires to participate as an approved laboratory in the Common Criteria Evaluation and Validation Scheme (CCEVS). COMPANY NAME recognizes that it must comply with both the requirements of the National Voluntary Laboratory Accreditation Program (NVLAP) for Information Technology Security Testing-Common Criteria Testing (NIST Handbooks 150 and 150-20) and the requirements of the CCEVS.</p> <p>COMPANY NAME hereby acknowledges there are requirements for participation within the CCEVS dictated by the scheme in addition to the NVLAP requirements. In order to be placed on the CCEVS Approved Laboratory List, COMPANY NAME acknowledges it must be accredited by NVLAP and comply with all of the requirements outlined in Publication #1, Organization, Management and Concept of Operations.</p> <p>COMPANY NAME, as of the date of this letter, is a legal entity, duly organized and incorporated, validly existing, and in good standing under the laws of the State of STATE NAME whose principal place of business is CITY, STATE.</p> <p>Point of contact for this application is POC NAME, TITLE, PHONE, E-MAIL ADDRESS.</p> <p>Sincerely,</p> <p>NAME TITLE</p>		

Annex E: Sample CCTL & CCEVS Non-Disclosure Agreement

NON-DISCLOSURE AGREEMENT

Proprietary Information

This Non-Disclosure Agreement, effective _____, is entered into by and between _____, with principal offices located at _____ (hereinafter referred to as _____) and The National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme (CCEVS). It is recognized that it will be necessary or desirable to exchange information between ___ and the CCEVS for the purpose of facilitating the oversight by the government of evaluation, performance of validation processes, and activities conducted by the parties pursuant to the CCEVS and, with respect to the information provided in a specific evaluation and validation, to limit the use of such information as necessary to perform that evaluation and evaluation oversight for the benefit of the evaluation sponsor (Sponsor) (hereinafter "Purpose"). With respect to the information exchanged between the parties subsequent to the effective date, the parties agree as follows:

- (1) "Proprietary Information" shall include, but not be limited to, performance, sales, financial, contractual and special marketing information, ideas, technical data and concepts originated by the disclosing party, and which the disclosing party desires to protect against unrestricted disclosure or competitive use, and which is furnished pursuant to this Non-Disclosure Agreement and appropriately identified as being proprietary when furnished.
- (2) To be protected hereunder, all Proprietary Information provided to the CCEVS must be clearly identified and properly marked by the ___ so that such Proprietary Information can be protected by the CCEVS to the full extent authorized by law. Proprietary Information provided by ___ to the CCEVS by a means other than writing, can be protected hereunder, so long as it is identified as proprietary at the time of transfer or is disclosed under circumstances that reasonably indicate that ___ considers it proprietary.
- (3) Each party covenants and agrees that it will keep in confidence, and prevent the disclosure to any person or persons outside its organization or to any unauthorized person or persons, any and all information which is received from the other under this Non-Disclosure Agreement and has been protected in accordance with paragraph 2 hereof; provided however, that a receiving party shall not be liable for disclosure of any such information if the same:
 - A. Was in the public domain at the time it was disclosed, or
 - B. Becomes part of the public domain without breach of this Non-Disclosure Agreement, or
 - C. Is disclosed with the written approval of the other party, or
 - D. Was independently developed by the receiving party without reference to the Proprietary Information disclosed hereunder, or

E. Is or was disclosed by the disclosing party to a third party without restriction, or

F. Is disclosed pursuant to the provisions of a court order or as otherwise required by law, provided that prompt written notice is given by recipient prior to any such disclosure, so that the disclosing party or owner of such Proprietary Information shall have an opportunity to seek appropriate protection from disclosure.

With respect to any Freedom of Information Act request, the CCEVS will actively solicit ___ assistance in establishing supportable bases for protecting such Proprietary Information. The CCEVS will not transfer or assign any Proprietary Information outside of the CCEVS without the prior written consent of ___.

As between the parties hereto, the provisions of this Paragraph 3 shall supersede the provisions of any inconsistent legend that may be affixed to said data by the disclosing party, and the inconsistent provisions of any such legend shall be without any force or effect.

Any Proprietary Information provided by one party to the other shall be used only in furtherance of the Purposes, and, subject to mandatory retention obligations, including but not limited to the record keeping requirements of the CCEVS and as otherwise required by law, shall be, within ten (10) days of the termination of the evaluation to which the Proprietary Information applies or upon request at any time, returned to the disclosing party or the receiving party will certify the destruction of any software or magnetic media. If either party loses or makes unauthorized disclosure of the other party's Proprietary Information, it shall notify such other party immediately and take all steps reasonable and necessary to retrieve the lost or improperly disclosed information.

(4) The standard of care for protecting Proprietary Information imposed on the party receiving such information will be that degree of care the receiving party uses to prevent disclosure, publication or dissemination of its own proprietary information but in no event less than a reasonable standard.

(5) In providing any information hereunder, each disclosing party makes no representations, either express or implied, as to the information's adequacy, sufficiency, or freedom from defect of any kind, including freedom from any patent infringement that may result from the use of such information, nor shall either party incur any liability or obligation whatsoever by reason of such information, except as provided under Paragraph 3, hereof.

(6) The receipt of Proprietary Information by the CCEVS for the purposes of performing government oversight of the evaluation shall not be construed in any way as a commitment to the Sponsor or the CCTL for any future procurement of any equipment or other terms of supply or service sold by the Sponsor or the 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 validators for the CCEVS will conduct the evaluation oversight. It is further understood and agreed that the CCEVS's 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 Non-Disclosure Agreement.

(8) Any report or other information provided by the CCEVS to the Sponsor and/or to ___ arising out of or as a result of this Non-Disclosure Agreement or the evaluation is not to be construed as an endorsement of the Sponsor's or ___ goods and/or services. The Sponsor and or ___ will not by advertising or otherwise claim or imply the existence of a CCEVS endorsement of its goods and/or services which are the subject of evaluation oversight pursuant to this Non-Disclosure Agreement.

(9) This Non-Disclosure Agreement contains the entire agreement relative to the protection of information to be exchanged hereunder, and supersedes all prior or contemporaneous oral or written understandings or agreements regarding this issue. This Non-Disclosure Agreement shall not be modified or amended, except in a written instrument executed by the parties.

(10) Nothing contained in this Non-Disclosure Agreement shall, by express grant, implication, estoppel or otherwise, create in either party any right, title, interest, or license in or to the inventions, patents, technical data, computer software, or software documentation of the other party or its suppliers, including but not limited to, the Sponsor. No modification of any kind of any Source Code or any other Proprietary Information is permitted pursuant to this Agreement without the prior written permission of ___. Specifically, the CCEVS agrees not to alter, remove or otherwise disturb any notices of intellectual or other proprietary rights, including without limitation, copyright. Except as necessary to conduct or validate an evaluation, the reverse engineering, decompilation or other source code derivation of any object code is specifically prohibited.

(11) Nothing contained in this Non-Disclosure Agreement shall grant to either party the right to make commitments of any kind for or on behalf of any other party without the prior written consent of that other party.

(12) The effective date of this Non-Disclosure Agreement shall be the date set forth in the opening paragraph above.

(13) This Non-Disclosure Agreement shall be governed and construed in accordance with federal statutes and regulations, notwithstanding any State conflict of law statutes, practices or rules of construction. To the extent that no federal law applies, the laws of the State of _____ shall govern, without giving effect to its conflict of laws provisions.

(14) This Non-Disclosure Agreement may not be assigned or otherwise transferred by either party in whole or in part without the express prior written consent of the other party, which consent shall not unreasonably be withheld. This consent requirement shall not apply in the event either party shall change its corporate name or merge with another entity. This Non-Disclosure Agreement shall benefit and be binding upon the successors and assigns of the parties hereto.

(15) This Non-Disclosure Agreement may be signed in counterparts, and delivered by facsimile, and such facsimile counterparts shall be valid and binding on the parties hereto with same effect as if original signatures had been exchanged.

NATIONAL INFORMATION
ASSURANCE PARTNERSHIP COMMON
CRITERIA EVALUATION AND
VALIDATION SCHEME

By: _____

By: _____

Name: _____

Name: Audrey M. Dale _____

Title: _____

Title: Director, CCEVS _____

Address: _____

Address: 9800 Savage Road, STE 6757 _____

Ft. Meade, MD 20755-6757 _____

Telephone No: _____

Telephone No: 410-854-4458 _____

FAX No: _____

FAX No: 410-854-6615 _____

Date: _____

Date: _____