National Information Assurance Partnership
Common Criteria/
Evaluation and Validation Scheme

Publication #4

Guidance to NIAP-Approved
Common Criteria Testing Laboratories

January 2020
Version 4.0

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

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

Amendment record

Version	Date	Description
1.0	20 March 2001	Initial release
2.0	8 September 2008	Complete revision based on current operations
3.0	28 August 2014	Updates
4.0	January 2020	Updates to reflect minor program changes

(This page intentionally left blank)

Table of Contents

1 Introduction

The Common Criteria Evaluation and Validation Scheme (CCEVS), hereafter referred to as The National Information Assurance Partnership (NIAP), Common Criteria Scheme, or Scheme, was originally established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to validate conformance of Information Technology (IT) products to international standards. NIAP, now solely part of NSA, oversees the evaluations performed by Common Criteria Testing Labs (CCTLs) on information technology products against the Common Criteria for Information Technology Security Evaluation (CC).

The principal participants in the NIAP program are the:

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

b) **Common Criteria Testing Laboratory (CCTL)**: The CCTL is a commercial testing laboratory accredited by NIST and approved by NIAP to perform security evaluations against the Common Criteria for Information Technology Security Evaluation (CC) using the Common Methodology for Information Technology Security Evaluation (CEM).

c) **National Information Assurance Partnership (NIAP**): NIAP is the government organization established by NSA 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 evaluation.

1.2 Organization and Scope

This document is one of a series of technical and administrative NIAP publications that describes how NIAP operates. It consists of several chapters and supporting annexes.

Chapter 1 provides a high-level overview of NIAP.
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, CCTL & NIAP Non-Disclosure Agreement, a glossary and a list of commonly used acronyms.

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

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

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

Publication #3: *Guidance to Validators*

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

Publication #5: *Guidance to Sponsors*

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

These publications, along with additional information, documents, and guidance are available on the NIAP web site at https://www.niap-ccevs.org/.

2 Common Criteria Testing Laboratory

Organizations interested in becoming a CCTL must go through a series of steps involving both NIAP and the National Voluntary Lab Accreditation Program (NVLAP). Rather than develop its own accreditation capabilities, NIAP has delegated the responsibility of CCTL accreditation to NVLAP, a subsidiary of NIST. Accreditation by NVLAP is the primary requirement for achieving CCTL status. NIAP 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
- Approved by NIAP
- Listed on the NIAP Approved CCTL List

NIAP has responsibility for the oversight of evaluations performed by CCTLs. In addition to technical oversight (validation) of every evaluation, NIAP 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

NIAP grants approval for candidate CCTLs to become a NIAP CCTL when all NIAP-specific and NVLAP accreditation requirements have been successfully met. Once all requirements have been met, the candidate CCTL is approved by NIAP to conduct IT security evaluations and is placed on the NIAP CCTL List.

2.1.1 NIAP-Specific Requirements

NIAP imposes the following NIAP-specific requirements[1]:

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]

[1] NIAP reserves the right to levy additional NIAP-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 NIAP as a CCTL. However, in order to meet the letter and spirit of the NIAP 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.

b) CCTL must perform all evaluation-related activities from the U.S. facility unless approved in advance by NIAP;

c) CCTL must agree to accept NIAP technical oversight and validation of evaluation-related activities in accordance with the policies and procedures established by the scheme;

d) 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 NIAP;

e) CCTL must be a third party independent evaluation facility that contains a demonstrated, fully operational security testing capability; and

f) CCTL must demonstrate technical and CC competencies as outlined in NIST Handbook 150-20, *Information Technology Security Testing—Common Criteria.*

NIAP will:

a) Verify the satisfaction of these requirements by confirming the content of the "Letter of Intent," submitted by a candidate CCTL (sample Letter of Intent);

b) Confirm and notify the CCTL of acceptance as a NIAP-approved CCTL when all NIAP-specific requirements and all NVLAP accreditation requirements have been met; and

c) Establish CCTL and NIAP agreement (Annex D).

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:

a) NIST Handbook 150[3], *Procedures and General Requirements*

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

[3] NIST Handbook 150 incorporates the requirements of ISO/IEC 17025, *General Requirements for the Competence of Calibration and Testing Laboratories*.

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.

A CCTL must ensure its NIAP approval and NVLAP accreditation remain current in order to maintain its status as a NIAP-approved testing laboratory. For the specific requirements for CCTLs during reaccreditation, see NVLAP Handbook 150 and 150-20.

2.2 Withdrawal or Suspension of Approval/Accreditation

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

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

If a CCTL has its NIAP approval or NVLAP accreditation *suspended* the CCTL must *temporarily* cease all NIAP 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-Approved CCTL will be withdrawn.

The conditions for withdrawal and suspension of NIAP approval and NVLAP accreditation are described in NIST Handbook 150 and NIST Handbook 150-20, Section 3.4.

2.3 Audits

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

2.4 Notifying NIAP of CCTL Operation Changes

A CCTL must notify NIAP 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. Some examples of events requiring written notification are a CCTL's intent to withdraw from NIAP, changes in ownership of a CCTL, or personnel changes in key staff positions. The above listed examples provide guidance on the types of changes

requiring written notification, but this list is not exhaustive. A CCTL should contact NIAP if clarification is needed about whether a change is significant enough to warrant written notification. Lack of written notification may result in suspension or withdrawal of NIAP approval.

2.5 Independence and Conflict of Interest

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

2.5.1 NIAP Conflict of Interest Guidelines

In order to avoid any actual or potential conflict of interest, the CCTL must agree 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 possibly resulting 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 developing and evaluating an IT product; or

b) providing consulting services that would compromise the independence of the evaluation to the sponsor of an evaluation or to the product developer.

Accordingly, CCTLs must ensure any activities related to the production of evaluation evidence in preparation for the evaluation (within that same testing laboratory) of an IT product do not conflict with the laboratory's ability to conduct a fair and impartial evaluation of that product. The scope of consulting work during the preparation for an IT security evaluation is not controlled by NIAP and is a matter of negotiation between the sponsor and the CCTL or other consultant. However, the CCTL must adhere to the terms and conditions of its NVLAP accreditation to ensure the advice given does not affect evaluator independence or impartiality in any evaluation. The CCTL must notify NIAP whenever any potential conflict of interest may occur. All CCTLs will be subject to the conflict of interest guidelines stated above. NIAP and NVLAP will verify these

conditions are met and will be the final arbitrators in determining potential or actual conflicts of interest threatening the integrity of security evaluations conducted within NIAP.

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 NIAP involvement.

2.6 Proprietary/Sensitive Information

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

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 security target (ST) and the associated IT product/system which 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 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 the ST meets NIAP minimum requirements for acceptance. NIAP Policy #12 provides guidelines for acceptance requirements of a product for NIAP Evaluation. These minimum requirements, explained below include Security Targets (STs) claiming exact compliance to a NIAP-approved PP. Once the CCTL has confidence the ST meets these minimum requirements, they should begin the ASE work units in preparation for submission to NIAP.

3.1 Acceptance of Security Targets (STs)

NIAP policies provide guidelines for acceptance of STs for evaluation. In particular, the product must claim exact compliance to a NIAP-approved Protection Profile. Additionally, the physical and logical boundary of the TOE must be described sufficiently to determine what is inside and what is outside the TOE.

3.2 Certification of NIAP-Approved Protection Profiles (PPs)

The Common Criteria mandates that all Protection Profiles and Protection Profile Configurations are evaluated. NIAP procedures dictate that this is performed on first use. A CCTL is responsible for performing all APE and ACE work units, as applicable, if there are no previously completed evaluations using the document(s). The results of these work units must be presented to NIAP as part of the evaluation results and be approved prior to evaluation completion.

4 Validation Process

4.1 Check-In/Check-Out Oversight Process

Due to the new paradigm in the NIAP scheme, NIAP is transitioning to a new oversight processes called 'Check-In/Check-Out.' In this process, NIAP will oversee the evaluation process by conducting periodic meetings in which those involved in the evaluation process will track progress and discuss issues within a specific evaluation.

The check-in/out process is designed to accommodate evaluations against NIAP-approved PPs, which are more objective and promote consistency in evaluations. Because NIAP-approved PPs have clearly defined, tailored assurance activities, it is anticipated that evaluation of products against the PPs will be accomplished more expeditiously. Products submitted for evaluation against a NIAP-approved PP are expected to have a sound Security Target and vendor-provided evidence that supports completion of all evaluation assurance activities delivered as part of the check-in package from the CCTL to NIAP. A complete check-in package mitigates the risk of delays during the evaluation and aligns with the goal of achievable, repeatable, testable, and timely NIAP evaluations. For a more comprehensive description of the Check-In/Check-Out process, please see NIAP Check-In/Check-Out Guidance.

4.2 TRRT

The mission of the Technical Rapid Response Team (TRRT) Process is to provide timely response to evaluation and protection profile technical issues raised throughout the course of an evaluation.

CCEVS assigns individuals to TRRTs for each technology type. Each team has a lead (or co-leads), and multiple members. The lead(s) is/are always drawn from the NIAP or validation community; other team members may be drawn from the validation community, the Technical Community (TC) responsible for the profile, and other technology experts for that technology. It is the responsibility of the lab/vendor to ensure identified issues are cleansed of any proprietary details before being transmitted to TRRT team members that are not part of the validation community (and thus not covered by non-disclosure agreements). We encourage involvement of the lab initiating the question as well as other entities (CCTLs, TCs, etc.) being part of the TRRT process.

An overview of the TRRT Process and submitting a TRRT inquiry can be found on the NIAP website.

4.4 ECR

The primary purpose of the Evaluation Consistency Review (ECR) is to ensure the technical consistency of the evaluation and validation processes against the PPs using a mix of validators to ensure different viewpoints on evaluations. During the ECR for each

evaluation, if the validation team recognizes the need for a PP update/clarification, they initiate a TRRT inquiry.

Additionally, the Technical Oversight Team holds periodic meetings to address and discuss common issues across multiple validations to provide varying perspectives on evaluations among a pool of validators.

5 Government Roles in Evaluation and Validation

Government evaluators are assigned as members of a CCTL evaluation team at the sole discretion of NIAP. 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 generally describes the responsibilities of these two NIAP representatives. For more information on the role of Validators, please see NIAP Publication #3.

5.1 Government Evaluators

The government evaluator (GE) is an individual assigned as a team member on an evaluation. The assignment is made at NIAP discretion in coordination with the CCTL 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 NIAP 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 NIAP and the CCTL and to ensure the evaluation meets NIAP 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 for evaluation-intense assurance activities. 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 NIAP to ensure the technical quality of the analysis performed. At the completion of the evaluation, the validator produces a Validation Report which provides an assessment of the evaluation process and the team's analysis.

At the discretion of NIAP, 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 check-in 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) in order to permit validation oversight. Exceptions to this location requirement may be granted on a case-by-case basis at the discretion of NIAP, 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 NIAP. For each evaluation, the CCTL must create an evaluation work plan for their quality system records. The work plan must include a list of assurance activities to be performed during the evaluation. As these assurance activities 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 Check-In/Check-Out 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 assurance activity must contain both the plan and the results of the work performed. The plan must include the objective of the assurance activity, the required inputs, and the techniques and tools that will be used to perform the activity.

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

5.4 Time Limits on NIAP Evaluations

An escalating complaint against NIAP 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 NIAP 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 NIAP Policy #18.

6 Concluding an Evaluation/Validation

The publication of the Product Compliant List entry and the issuance of the certificate conclude an evaluation/validation.

Upon completion of the evaluation analysis, the CCTL will provide the Validator with all documentation required by the CICO guide. The ETR should be complete, including proprietary and/or sensitive information.

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

The NIAP Director will make the decision to either:

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

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

The contents of a CC certificate are described in Publication #1, *Organization, Management and Concept of Operations*. There are rules associated with the use of the NIAP certificate and the CC Certification Mark. See Publication #5 for the CC Certification Mark Usage Policy.

Annex A: References

Common Methodology for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017.

Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017.

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

NIST Handbook 150:2016 Edition, *Procedures and General Requirements*

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

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
ECR	Evaluation Consistency Review
ETR	Evaluation Technical Report
ISO	International Organization for Standardization
NIAP	National Information Assurance Partnership
MR	Memorandum for Record
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TRRT	Technical Rapid Response Team
VID	Validation Identification
VR	Validation Report

Annex C: Glossary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Laboratory Accreditation Program (NVLAP) and NSA is responsible for the National Information Assurance Partnership (NIAP).

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

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

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

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

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

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

Technical Rapid Response Team (TRRT): A panel composed of scheme validators to ensure technical consistency across evaluations and validations performed under NIAP.

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

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

Annex D: Sample CCTL & NIAP 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: _____
Title: _____	Title: Director, NIAP _____
Address: _____	Address: 9800 Savage Road, STE 6940
_____	Ft. Meade, MD 20755-6940
Telephone No: _____	Telephone No: 410-854-4458
FAX No: _____	FAX No: 410-854-6615
Date: _____	Date: _____