National Information Assurance Partnership /Common Criteria Evaluation and Validation Scheme

Publication #1

Organization, Management, and Concept of Operations

March 2016
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
http://www.niap-ccevs.org/

Amendment record

Version	Date	Description
2.0	May 1999	Initial release.
2.0	September 2008	Complete revision based on current operations. The version number remained 2.0 to be consistent across all publications updated in 2008.
3.0	February 2014	Updates
4.0	March 2016	Updates

(This page intentionally left blank)

Table of Contents

1 Introduction

This document is intended to provide an overview of the National Information Assurance Partnership (NIAP) to all interested parties, including Information Assurance (IA) and IA-enabled Information Technology (IT) sponsors, product developers or vendors, Common Criteria Testing Laboratories (CCTLs), and consumers of evaluated products.

Security concerns are motivated by an increasing use of IA and IA-enabled IT products and systems in areas, from electronic commerce to national defense. Consumers have access to a growing number of security-enhanced IT products with different capabilities and limitations, and must make important decisions to select the best products that provide the appropriate degree of protection for their information.

Although the National Security Agency (NSA) strategy for protecting classified information may employ traditional Government Off-The-Shelf (GOTS) IA solutions, the NSA Information Assurance Directorate (IAD) first looks to commercial technology and commercial solutions that help meet customers' needs for protecting classified information.

In order to help consumers select appropriate Commercial Off-The-Shelf (COTS) IA and IA-enabled IT products and help manufacturers of those products gain acceptance in the global marketplace. NSA, in partnership with The National Institute of Standards and Technology (NIST) manages and maintains a program to evaluate IA and IA-enabled IT product conformance to international standards. This program is titled the Common Criteria Evaluation and Validation Scheme, (CCEVS) – hereafter referred to as The NIAP, Common Criteria Scheme, or Scheme.

NIAP only accepts products into evaluation that claim exact compliance to a NIAP-approved Protection Profile. These NIAP-approved Protection Profiles (PP) produce evaluation results that are achievable, repeatable, and testable – allowing for more a more consistent and rapid evaluation process.

1.1 Objectives

The primary objectives of NIAP are to:

a. Ensure security evaluations of IT products are performed to consistent standards and each evaluation is achievable, repeatable, and testable;

b. Meet the needs of government and industry for cost-effective evaluations of IT products;

c. Improve the availability of evaluated IT products; and

d. Encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry.

NIAP serves many communities of interest with very diverse roles and responsibilities, including product developers and vendors for a broad spectrum of technology areas,

product evaluators, and procurers from across the U.S. government and internationally. Close cooperation between government and industry is paramount to the success of the Scheme. To this end, NIAP forms and manages Technical Communities (TC) to create, maintain, and update Protection Profiles (PP) for key technology areas. These communities are composed of IT product developers, product vendors, value-added resellers, systems integrators, IT security researchers, acquisition/procurement authorities, consumers of IT products, auditors, and system accreditors.

Subject Matter Experts (SMEs) within the TCs are empowered to advocate for changes of content within their corresponding PPs. Domain experts provide threat information and Security Functional Requirements (SFRs).

Note: Only those capabilities that support government needs and are required to counter technology-specific threats are included as SFRs within a PP. Assurance activities are carefully crafted by SMEs in order to produce results that can be repeated across technology areas, and to ensure Security Assurance Requirements are appropriate for the technology and meet government's needs.

1.2 Evaluation and Validation of COTS Products

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

Consumers of IT products require confidence in the security features of procured products. Consumers could gain confidence in a particular IT product by testing each prospective product directly and obtaining the necessary measurable results. Alternatively, consumer confidence in a particular IT product can be based on the trusted reputation of the developer, past experience with the developer, or the developer competence in building products demonstrated through recognized assessments. The first approach requires substantial, costly duplication of effort while the other approaches are ad hoc and lack measurable results.

The NIAP Common Criteria Scheme overcomes these limitations and enables consumers to obtain an impartial assessment of an IT product by an independent entity. This impartial assessment, or security evaluation, includes analyzing and testing the product for conformance to a defined set of security requirements. The IT product being evaluated is referred to as the Target of Evaluation (TOE). The set of security requirements for that product are defined in the product's Security Target (ST). IT security evaluations are composed of analysis and testing.

In order for consumers and industry to have confidence in the results of IT product security evaluations, it is important that those evaluations conform to recognized standards and procedures, and be objective. The use of standard IT security evaluation criteria, IT security evaluation methodology, and Protection Profile assurance activities

contribute to the repeatability and objectivity of the results but are sufficient for a comprehensive, objective evaluation. Many of the evaluation criteria also require the judgment and background knowledge of technical subject matter experts. Because differing technologies have differing SMEs, consistency in these judgment calls is, more difficult to achieve. In order to provide independent confirmation that an IT security evaluation was conducted in accordance with the provisions of the Scheme and that the conclusions of the testing laboratory are consistent with the facts presented in the evaluation, the final evaluation results are validated to provide independent confirmation that an IT security evaluation was conducted in accordance with the provisions of the Scheme. This final validation, is intended to promote consistency of IT security evaluations and comparability of results across all evaluations conducted within the Scheme.

The impartial evaluation, the independent validation of the evaluation results, and the documentation resulting from those processes provides valuable information for consumers about the security capability of IT products. However, consumers will still need to review this information carefully and assess its applicability to local needs, (e.g., the situation and operating environment in which the product will actually be used). Section 3.4 of this document provides additional guidance to consumers of IT products regarding the specific use of security evaluation results.

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

1.3 Historical Perspective

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

Beginning in the 1980s, NIST and NSA promoted security in COTS IT products. Their efforts focused on government-sponsored initiatives to produce effective IT security evaluation criteria, (e.g., the Trusted Computer System Evaluation Criteria [DOD85] and the Federal Criteria for Information Technology Security), and to evaluate products developed by industry in response to those criteria. The development of similar IT security evaluation criteria by Canada and several European nations and recognition of the increasing world-wide markets for U.S. manufacturers of IT products prompted the effort to harmonize existing evaluation criteria into “Common Criteria” (CC)—internationally accepted and standards-based. The Common Criteria was established in 1997 as the result of a multi-year effort by the governments of the United States, Canada,

United Kingdom, France, Germany, and the Netherlands to develop harmonized security criteria for IT products. In 1998, version 2.1 of the CC was accepted by the International Organization for Standardization (ISO) as an international standard, ISO/IEC 15408, The Common Criteria for Information Technology Security Evaluation.
At the same time the CC was being developed, there was a parallel effort to transition trusted product evaluations from the government to the private sector. NSA began the transition of its commercial IT product evaluation capability, (i.e., the Trusted Product Evaluation Program) to the private sector with the establishment of the Trust Technology Assessment Program (TTAP). Under this program, IT security evaluations were conducted by commercial testing laboratories using the NSA evaluation methodology in accordance with cooperative research and development agreements. The transition continued under NIAP when commercial testing laboratories began conducting CC-based evaluations of IA and IA-enabled IT products on a fee-for-service basis using the Common Evaluation Methodology.

The NIAP has grown substantially since its 2000 inception, from managing just a few accredited commercial testing laboratories and having a handful of products evaluated, to overseeing numerous CCTLs and successfully completing hundreds of evaluations.

NIAP evaluations have been significantly shortened within the past few years from an open-ended evaluation schedule to a 90-day evaluation paradigm. As a result, the NIAP Product Compliant List grew over 500% from 10 products in late 2013 to nearly 100 two years later.

1.4 Scheme Publications

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

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 http://www.niap-ccevs.org/.

2 Overview of the Scheme

The principal participants in the Scheme are as follows:

Sponsor: The sponsor may be a product developer, but could also be a government agency, industry consortium, or other organization seeking to obtain an IT security evaluation. A sponsor is the party requesting and paying for the security evaluation of an IT product by an accredited testing laboratory.

Common Criteria Testing Laboratory (CCTL): The CCTL is a commercial testing laboratory accredited by National Institute of Standards and Technology (NIST) and approved by NIAP. The NIST *National Voluntary Laboratory Accreditation Program (NVLAP)* plays an essential role in supporting Scheme requirements for laboratory accreditation by ensuring that laboratories meet accreditation requirements defined in NIST Special Publication 150-20, *Common Criteria Testing*.

National Information Assurance Partnership (NIAP): The NIAP is a U.S. Government organization, managed by NSA, established to maintain and operate the Scheme for the U.S. Government. Operating in the interest of both the public and private sectors, the NIAP approves participation of security testing laboratories in the Scheme, in accordance with its established policies and procedures. It also provides technical guidance to those testing laboratories, validates the results of IT security evaluations for conformance to the CC, and serves as an interface to other nations on the mutual recognition of such evaluations.

Technical Community (TC): TCs are government/industry partnerships formed to:

a. Develop CC Protection Profiles (PPs) to address evaluations of specific groups of commercial products;

b. Ensure PP content reflects the current state and best practices for the secure use of identified technologies; and

c. Influence the evolution of identified technologies to ensure they are able to satisfy government protection needs in the face of changing threats.

TCs is to ensure PPs are generated through collaboration between Government and industry groups --that leverage and share their knowledge of the threats and vulnerabilities for particular technologies. Those industry groups are responsible for building and commercializing the technologies. This collaboration is designed to improve the state of security for commercial products and continuously integrate emerging security capabilities and practices over time. TCs are responsible for the following PP content:

a. A set of technology-specific threats derived from operational knowledge and technical expertise,

b. The minimal security functionality sufficient to mitigate the identified threats; and

c. A collection of assurance activities tailored to the technology and covering each functional requirement. These activities are required to be objective, testable, measurable, repeatable, and scoped such that they can be completed within a reasonable time-frame.

In order for a testing laboratory to obtain accreditation and ultimately CCTL status, it must complete a series of steps involving both the NIAP Validation Body and the NIST NVLAP. Accreditation by NVLAP is the primary requirement for a laboratory to obtain CCTL status. A laboratory must meet the requirements of NIST Handbooks 150 and 150-20. Three Scheme-specific requirements are imposed by the NIAP Validation Body. NIAP approved CCTLs must:

a. Reside within the U.S. and be a legal entity, duly organized and incorporated, validly existing, and in good standing under the laws of the state where the laboratory intends to do business;

b. Agree to accept U.S. Government technical oversight and validation of evaluation-related activities in accordance with the policies and procedures established by the NIAP Common Criteria Scheme;

c. Agree to accept U.S. Government participants in selected Common Criteria evaluations conducted by the laboratory in accordance with the policies and procedures established by the NIAP Common Criteria Scheme.

Once NVLAP accreditation is received and any additional Scheme-specific requirements are met, the CCTL is placed on the NIAP *Approved Common Criteria Testing Laboratories (CCTLs) List*. Specific details regarding NVLAP accreditation, re-accreditation, expansion of scope, and the CCTL approval process can be found in Publication #4: *Guidance to CCEVS Approved Common Criteria Testing Laboratories*.

NIAP validates the results of all security evaluations conducted by a CCTL within the Scheme and, when appropriate, issues a CC certificate. The certificate, together with its associated validation report, confirms that an IT product has been evaluated for conformance to the CC at an accredited testing laboratory using the Common Criteria Evaluation Methodology (CEM). The certificate also confirms the IT security evaluation has been conducted in accordance with the provisions of the Scheme and that the conclusions of the CCTL are consistent with the evidence presented during the evaluation.

The NIAP maintains a *Product Compliant List (PCL)* of all IA and IA-enabled IT products that have successfully completed evaluation and validation under the Scheme. A list of products that are in the evaluation process is also maintained by NIAP. The names of products on this *Products in Evaluation* list are subject to approval by the evaluation sponsor. Some sponsors do not wish to disclose this information until the product has received a CC certificate and can be posted to the PCL. In order for IT products to receive CC certificates and be placed on the NIAP PCL, evaluations must be performed

using NIAP-approved processes. The PCL and *Products in Evaluation* lists are located on the NIAP web site at http://www.niap-ccevs.org.

The cost of an IT security evaluation is determined by the individual contract negotiations between the sponsor of the evaluation and CCTL selected to conduct the evaluation. NIAP does not play a role in sponsor-laboratory contract negotiations, does not monitor costs, and does not provide CCTL referrals. NIAP does not charge sponsors for validation services.

3 Roles and Responsibilities

This chapter describes the roles and responsibilities of the principal participants in the Common Criteria Scheme.

3.1 Sponsor of an IT Security Evaluation

The *sponsor* is the individual or organization requesting a security evaluation of an IT product. The relationship of the sponsor to the IT product may vary, depending on the nature of the product and the circumstances surrounding the evaluation. In most cases, the sponsor of a security evaluation will be the actual developer of the IT product. However, the sponsor may be a value-added IT product reseller or an organization or individual acquiring an IT system in which that particular product as a key component.

When the sponsor is not the product developer, the sponsor must ensure the developer cooperates in providing the CCTL with technical materials and essential deliverables necessary to conduct the IT security evaluation in a complete and consistent manner. The developer's incentive to cooperate in providing needed materials is sale of their product to the sponsor. Contractual agreements between the sponsor and the IT product or PP developer must include the specific details for providing the required documentation. The guidance to evaluation sponsors are outlined in Publication #5: *Guidance to Sponsors of IT Security Evaluations.*

3.2 NIAP

The principal objectives of NIAP are to ensure competent IT security evaluation and validation services are provided for both government and industry. NIAP is ultimately responsible for the operation of the Scheme in accordance with its policies and procedures and, where appropriate, for the interpretation and amendment of those policies and procedures. NSA is responsible for providing sufficient resources to NIAP to carry out its responsibilities.

NIAP CCEVS is led by a Director, selected by NSA management. The NIAP Director reports to an NSA organization designated to oversee NIAP. Technical and administrative support personnel provide a full range of validation services for the sponsors of evaluations and the CCTLs. These personnel include validators, technical experts, and senior members of the technical staff.

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

For additional details, see Publication #2: *Quality Manual and Standard Operating Procedures.*

NIAP is responsible to:

a. Establish and implement policies and procedures for the operation of the Scheme, and to ensure these policies and procedures are adhered to;

b. Document and publicize the organization, policies, and procedures of the Scheme;

c. Approve each CCTL to participate in the Scheme and publicize the approved CCTLs on the NIAP-Approved Laboratories List;

d. Monitor the performance of participating CCTLs to ensure they adhere to, apply and interpret the CC Scheme, CEM, and PPs;

e. Remove a CCTL from the NIAP-Approved Laboratories List if the laboratory fails to meet the terms and conditions of the Scheme;

f. Notify to the community (i.e., industry and government stakeholders) of any changes to the NIAP-Approved Laboratories List, including additions or withdrawals of CCTLs from the Scheme and any modifications to the scope of a laboratory's accreditation;

g. Ensure appropriate procedures are in place within the Scheme to protect sensitive or proprietary information relating to IT products under evaluation and that those procedures are routinely followed;

h. Provide advice, guidance, support, and standards for training to CCTLs as required;

i. Review evaluation technical reports from CCTLs to ensure the conclusions are consistent with the evidence presented and that the CC, the Common Evaluation Methodology, and PPs have been correctly applied;

j. Facilitate the development of Protection Profiles by Technical Communities, thereby ensuring consistency of all CCTL evaluations across the scheme.

k. Seek guidance from industry experts (e.g., consumer groups, IT product technical community, testing laboratories, researchers, standards groups) when resolving disputes, addressing challenges, answering technical questions or making critical decisions regarding any aspect of the Scheme;

l. Issue CC certificates for products successfully evaluated and validated by the Scheme;

m. Publish and maintain a PCL of all successfully evaluated and validated products, along with their respective security targets and validation reports;

n. Promote the integrity of the CC certificates and ensure the CC and NIAP logos are used correctly;

o. Ensure the interests of all parties participating in Scheme activities are given appropriate consideration;

p. Arbitrate disputes arising in the context of the Scheme and provide procedures for appeal or reconciliation;

q. Approve press releases or similar statements relating to the Scheme;

r. Maintain a record system for creating, storing, accessing, archiving and disposing of Scheme records used to document NIAP activities;

s. Work with the U.S. Government policy offices (Department of Defense, Committee on National Security Services, etc.) to ensure policies are in concert with the NIAP and the international CC scheme known as the Common Criteria Recognition Arrangement.(CCRA);

t. Author and promulgate protection profiles;

u. Prioritize, establish, lead, and manage technical communities created to develop, modify, or update PPs; and

v. Liaise with international Schemes to ensure a robust collection of evaluated products and a consistent way forward within the CCRA.

Publication #2, *Quality Manual and Standard Operating Procedures*, outlines Specific requirements for the NIAP.

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

3.3 Common Criteria Testing Laboratories

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

- NIST Handbook 150, Procedures and General Requirements;
- NIST Handbook 150-20, Information Technology Security Testing - Common Criteria; and,
- Specific criteria for IT security evaluations and other requirements of the Scheme, as defined by the NIAP (see Publication #4, Guidance to CCEVS Approved Common Criteria Testing Laboratories).

CCTLs enter into contractual agreements with sponsors to conduct security evaluations[1] of IT products and protection profiles using NIAP-approved test methods derived from the CC, CEM and other technology-based sources. The IT security evaluations are carried out in accordance with the policies and procedures of the Scheme.

CCTLs must observe the highest standards of impartiality, integrity, and commercial confidentiality; and operate within the guidelines established by the Scheme. CCTLs must have documented policy and procedures to ensure the protection of sensitive or proprietary information. These procedures are subject to audit by NVLAP and the NIAP.

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. The term "ownership interest" shall include any percentage of ownership that is greater than 5%. Other prohibited relationships include, but are not limited to, instances where the CCTL has entered into an agreement that would result in the CCTL directly benefiting financially from the commercial sale of the product being evaluated or where the CCTL has sole distributorship rights for the evaluated product.

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

- Both the development and the evaluation of an IT product;
- Providing consulting services to the evaluation sponsor or a product/profile developer, which could compromise the independence of the evaluation.

Accordingly, CCTLs must ensure that any activities related to the production of evaluation evidence for a particular IT product about to enter evaluation (within that same testing laboratory) do not conflict with the laboratory's ability to conduct a fair and impartial evaluation of that product or profile. The above conflict of interest guidelines are subject to audit by NIAP and NVLAP to ensure these conditions are met. NIAP and NVLAP are the final arbiters in determining potential or actual conflicts of interest that may threaten the integrity of security evaluations conducted within the Scheme.

A CCTL must provide the NIAP with 30 days' notice of its intention to withdraw from the Scheme. Additional information pertaining to CCTLs can be found in Publication #4: *Guidance to Common Criteria Testing Laboratories*.

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

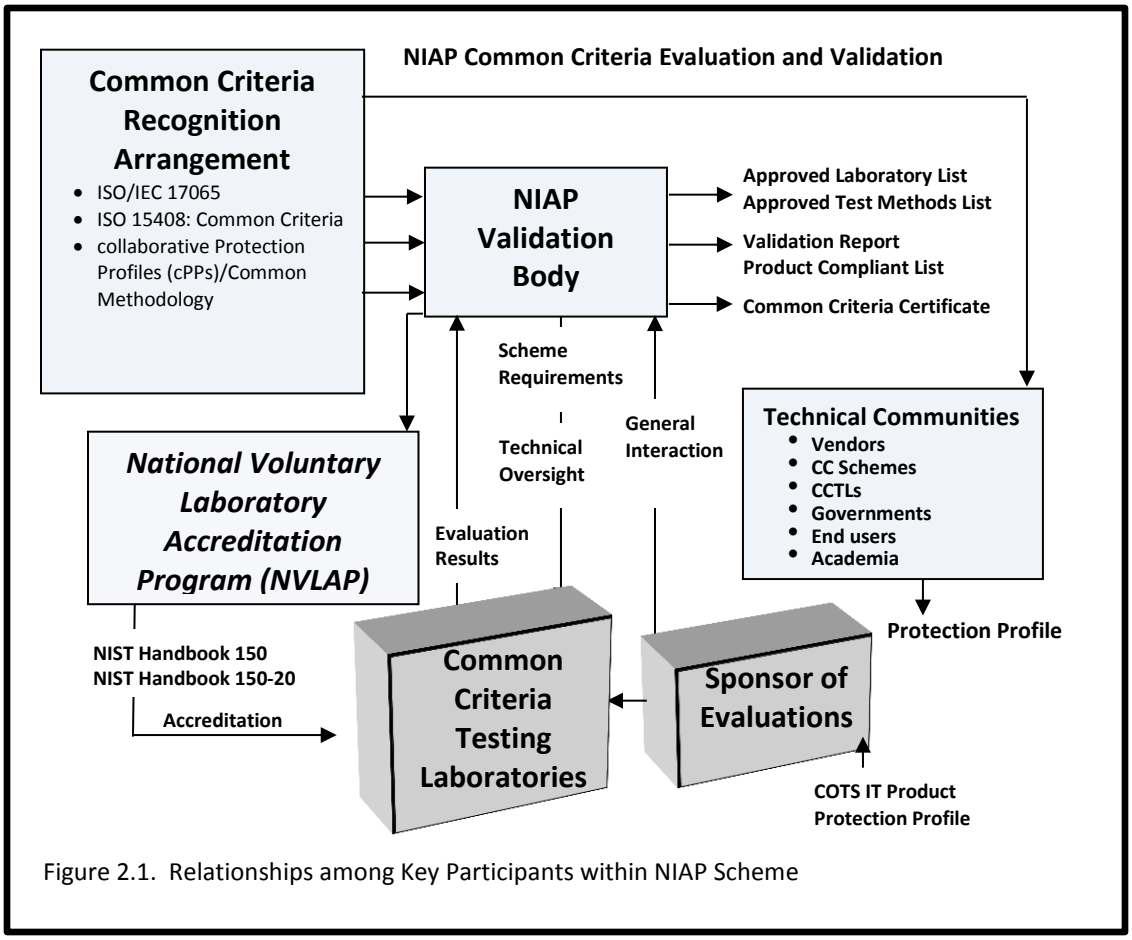

Figure 2.1. Relationships among Key Participants within NIAP Scheme

3.4 Guidance for Consumers

It is important for IT product consumers to understand how to interpret the results of IT security evaluations conducted within the Scheme. These results are described in evaluation technical reports produced by the CCTLs and summarized in the associated validation reports and CC certificates published by the NIAP.

An IT product is typically evaluated in a generic laboratory setting at a CCTL within the Scheme. Some general assumptions are made about the operational environment where the product will ultimately be deployed once the evaluation has been completed. In some cases, an evaluated IT product may be integrated into a more complex configuration of products that compose an IT system. The actual environment may also be significantly different from the one described in the original assumptions described in the document that defines the security functions and the operating environment known as the *Security Target*. (See Section 4.1.2 for a detailed description of a Security Target) In the end, consumers must assess the overall contribution to assurance made by the evaluated IT product. A product listed on the NIAP PCL alerts the consumer that the product has been successfully evaluated. The PCL should be the first point of reference when considering products to procure. Consumers should consider several things when assessing the suitability of the product to their circumstances:

- The accuracy and completeness of security evaluation results are dependent on the accuracy and completeness of the information and documentation provided to the CCTL by the sponsor of the evaluation;
- The quality of evaluation evidence and results are a function of how well the product is able to be described under the CC and the degree to which the Protection Profiles, Common Methodology, and the derivative test methods can measure conformance to the assurance activities specified to meet the security requirements;
- The security evaluation results are only for the product in its evaluated configuration. Consumers are responsible for determining the security impact of installing or operating an evaluated IT product in a configuration other than the configuration in which it was evaluated.

4 Evaluation and Validation of COTS Products

This chapter describes the activities of the Common Criteria Scheme participants during the various stages of a COTS product security evaluation.

In order to verify that a PP is sound and internally consistent, the PP must be evaluated before it is finalized. NIAP performs evaluation of all PPs as part of the first product evaluation against the PP. Upon successful completion of a product evaluation against the PP, the PP is considered evaluated for the purposes of Mutual Recognition under the CCRA and is listed on the CC portal web site. All partnering Schemes recognize the PP is evaluated per the CCRA Mutual Recognition Agreement.

4.1 Preparation for IT Security Evaluation

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

4.1.1 Consulting Work in Support of Evaluations

Common Criteria evaluation consultants may be hired by the sponsor to assist in preparing for an evaluation (e.g., reviewing and preparing evaluation evidence, assisting in resolving evaluation issues, etc.). Hiring an evaluation consultant is not required. Consultants may work for a CCTL, or be independently employed. The sponsor is solely responsible to decide on whether to hire a consultant and whom to hire and NIAP is never involved in this decision. The scope of consultant work during the preparation for an IT security evaluation is not controlled by the Scheme and is a matter for negotiation between the sponsor and the consultant. However, if the CCTL is used for consulting, the Laboratory must adhere to the terms and conditions of its NVLAP accreditation and NIAP conflict of interest guidelines to ensure that any advice does not affect evaluator independence or impartiality in any evaluation.

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

4.1.2 Security Target (ST)

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

4.1.3 Deliverables to CCTL

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

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

4.1.4 Readiness for Evaluation

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

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

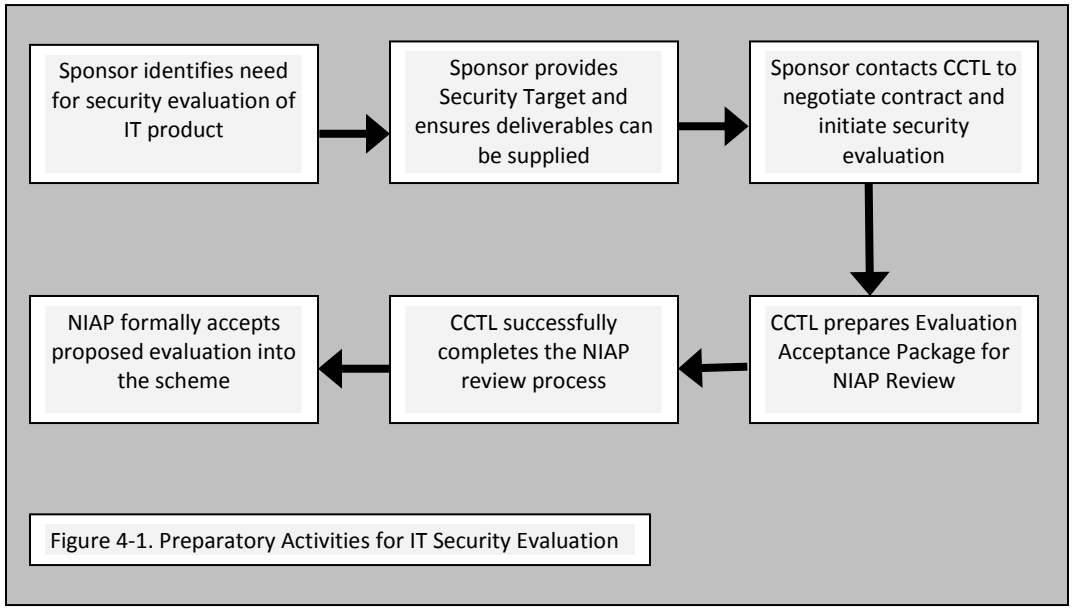

Figure 4-1. Preparatory Activities for IT Security Evaluation

4.2 Technical Oversight

NIAP only conducts evaluations against NIAP-approved PPs. The activities documented in PPs ensure all evaluations are achievable, repeatable, and testable; and scoped so that they can be completed within a reasonable time-frame. In addition, the evaluation and validation activities taking place within the Scheme will be conducted in accordance with the provisions of the Common Criteria, the Common Methodology, and the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security*, and any Scheme-specific policies and procedures. Technical oversight involves the monitoring of CCTLs and the review of specific evaluations.

NIAP must assign a technical representative, or *Validator*, to each IT security evaluation to serve as the primary point of contact for the CCTL and sponsor of the evaluation. The CCTL and sponsor must also assign a point of contact to interact with the NIAP during the evaluation. NIAP must have its technical representative monitor the evaluation and perform a variety of validation activities as described in Publication #3: *Guidance to Validators.*

4.2.1 CCTL Accreditation and Monitoring

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

Technical oversight includes monitoring the CCTLs. NIAP staff ensures consistency among CCTLs through frequent contact with CCTL personnel, CCTL meetings, written guidance issuances called *labgrams*, etc.

NIAP validators monitor CCTLs during each evaluation in two ways:

1. Ensuring the CCTL is following the Laboratory's documented quality processes (i.e., conflict of interest policies, record-keeping processes, evaluator training processes, etc.) and
2. Performing Validation Oversight Reviews /Check-In/Check-Outs to ensure the technical soundness of the work performed by the evaluation team (i.e., correct application of the CC, technical accuracy of the evaluation analysis, thorough testing during the evaluation, etc.).

4.2.2 Scope of Technical Oversight

NIAP provides oversight, as required, to adequately ensure that the CCTL has correctly and completely applied the Common Criteria and the Common Methodology for the specific IT security evaluation. The purpose of evaluation monitoring is to mitigate risk among all participants in the Scheme, (i.e., the NIAP, CCTLs, and sponsors). The

number, type, and intensity of activities associated with the oversight process will be a function of:

- The intricacy of assurance requirements that appear in the PP;
- The complexity of the TOE; and
- The experience of the CCTL in evaluating IT products in the identified technology area.

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

4.3 Conduct of the IT Security Evaluation and Validation

Evaluation is the assessment of an IT product for conformance to the CC. The objective is to enable the evaluating CCTL to prepare and impartially report whether the TOE satisfies its security requirements. This process, titled "Check In/Check Out" provides independent confirmation that an IT security evaluation has been conducted in accordance with the provisions of the Scheme and that the conclusions of the CCTL are consistent with the facts presented in their Evaluation Technical Report. The specific details of the technical oversight process and activities associated with it are described in Publication #3, *Guidance to Validators*.

5 Common Criteria Certificates

Once NIAP has approved the final validation report, NIAP will issue a Common Criteria Certificate for the evaluated IT product. NSA is the certificate-issuing authority for the NIAP. The Director of NIAP and a senior executive from NSA sign the certificate, indicating acceptance of the aforementioned criteria. After NIAP has issued the Certificate, NIAP Product Compliant List will be updated to include the product that was issued the Certificate.

5.1 Proper Use of CC Certificate

The Certificate applies only to the specific version and release of the IT product in its evaluated configuration. A sponsor must only market an IT product as an evaluated product, based on the validation report and accompanying Common Criteria (CC) Certificate published by NIAP. To ensure secure products, the sponsor must initiate the assurance maintenance process after the Certificate has been issued. This process requires reevaluation of the IT product if the vendor has made a major change. Additional details on the assurance maintenance process are described in Publication #6 *Assurance Continuity: Guidance for Maintenance and Re-evaluation.*

The issuance of a CC Certificate does not imply endorsement of an IT product by NIAP, NSA, or any other agency of the U.S. Government. Additional details on Common Criteria certificates can be found in Publication #2 *Quality Manual and Standard Operating Procedures* and Annex D.

5.2 Certificate Maintenance

Procedures for the maintenance of Common Criteria certificates, (e.g., in conjunction with extensions to later releases or versions of the IT product), are governed by the Common Criteria Certificate Maintenance Program as described in Publication #6: *Assurance Continuity: Guidance for Maintenance and Re-evaluation*. Assurance Continuity for an IT product is required every two years per NIAP Policy. Depending on whether the product has had significant changes within this time-frame, the product may require re-evaluation. NIAP determines whether or not a change requires re-evaluation...

A sponsor, anticipating the need for re-evaluation, may wish to consider a certificate maintenance approach at early stages of the initial evaluation in order to minimize future evaluation activities. Sponsor coordination with a CCTL may be required in order to take re-evaluation or certificate maintenance requirements into account when performing the initial evaluation of the IT product. Specific details of the certificate maintenance process employed within the Scheme are provided in Publication #6: *Assurance Continuity: Guidance for Maintenance and Re-evaluation.*

Annex A: References

Current versions of the CC/CEM, Common Criteria for Information Technology Security Evaluation.

Current versions of the NIST Handbook 150, *NVLAP Procedures and General Requirements* and *NVLAP Common Criteria Testing*.

DOD85, DoD 5200.28-STD –Department of Defense Trusted Computer System Evaluation Criteria, 26 December 1985.

ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, 2009.

ISO/IEC 17065:2012 — Requirements for Bodies Certifying Products, Processes, and Services, 2012.

ISO/IEC Guide 2:2004 – (formerly ISO Guide 2) – Standardization and related activities – General vocabulary, 2004.

Annex B: Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCMB	Common Criteria Maintenance Board
CEM	Common Evaluation Methodology
CCRA	Common Criteria Recognition Arrangement
CCTL	Common Criteria Testing Laboratory
CICO	Check-In/Check-Out
COTS	Customer Off-The-Shelf
ETR	Evaluation Technical Report
GOTS	Government Off-The-Shelf
IAD	Information Assurance Directorate
ISO	International Organization for Standardization
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PCL	Product Compliant List
PP	Protection Profile
SFR	Security Functional Requirements
SME	Subject Matter Experts (or Expertise)
ST	Security Target
TC	Technical Community
TOE	Target Of Evaluation
TTAP	Trust Technology Assessment Program
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 terms in ISO Guide 2 and are also broadly consistent with the CC and CEM.

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 that can be selected by a CCTL in choosing its scope of accreditation; that is, the types of IT security evaluations that the CCTL will be authorized to conduct using NIAP-approved test methods. This list of approved test methods is maintained by NIAP.

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 that 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 CC certificate. This process by provides a means (through specific assurance maintenance requirements) to ensure that a validated TOE continues to meet its ST as changes are made to the IT product or its environment.

Assurance Continuity Maintenance Report: A publicly available report that describes all changes made to the validated TOE which has 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.

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 that confirms an IT product or PP has successfully completed evaluation by an accredited CCTL in conformance with the CC standard.

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

Common Criteria Recognition Arrangement (CCRA):

Common Criteria Testing Laboratory (CCTL): An IT security testing laboratory that, , is accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by NIAP to conduct Common Criteria-based evaluations within the context of the Common Criteria Evaluation and Validation Scheme.

Common Evaluation Methodology (CEM): Common Methodology for Information Technology Security Evaluation: the formal title of a technical document that 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 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 between the NIST and the NSA that established a program to evaluate IT product conformance to international standards. NIST is responsible for the NVLAP and NSA is responsible for the NIAP.

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

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

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 set of software, firmware, and/or hardware, sometimes accompanied by guidance.

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

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

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

Annex D: Common Criteria Certificates

The following information must be included on all Common Criteria Certificates issued by the NIAP. The mutual recognition mark (logo) and [INSERT name of other logo on certificate) must be placed on each Common Criteria certificate issued by the NIAP, in addition to the information. The certificate is only valid in conjunction with the full validation report produced for its associated IT product or protection profile evaluation.

A Common Criteria Certificate issued by the NIAP, resulting from the validation of an IT product evaluation, shall include the following information:

a) Product developer;

b) Product name;

c) Version and release numbers;

d) Protection Profile identifier (if claiming conformance);

e) Evaluation platform (if applicable);

f) Name of CCTL;

g) Validation report number;

h) Date issued;

i) Signature of Director, Common Criteria Evaluation and Validation Scheme, National Information Assurance Partnership;

j) Signature of Information Assurance Director, National Security Agency;

k) A statement indicating that:

1) The IT product has been evaluated at an accredited testing laboratory using the Common Methodology for Information Technology Security Evaluation (version number) for conformance to the Common Criteria for Information Technology Security Evaluation (version number) as articulated in the product's functional and assurance security specification contained in its security target;

2) The evaluation has been conducted in accordance with the provisions of the Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consist with the evidence presented;

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

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

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

National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Company Name

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

Product Name:
Version:
Evaluation Platforms:

CCTL:
Validation Report Number:
Date Issued:
Protection Profile Identifier:
Assurance Level:

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

Information Assurance Director
National Security Agency

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