National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

McAfee HIP 6.0.2 and ePolicy Orchestrator 3.6.1 patch 1

Report Number: CCEVS-VR-07-0030

Dated: 17 May 2007

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Jerome F. Myers
David M. Dignan

Common Criteria Testing Laboratory
COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

List of Figures

List of Tables

EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the McAfee HIP 6.0.2 and ePolicy Orchestrator 3.6.1 patch 1 at EAL3. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on 5 March 2007. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.3, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 3 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the McAfee HIP and ePolicy Orchestrator that consists of a set of software components executed on Windows platforms. The TOE is comprised of two parts: the McAfee HIP agent and the ePolicy Orchestrator. McAfee HIP and ePolicy Orchestrator collectively is a Host Intrusion Protection tool and management tool intended for use in networked environments.

HIP 6.0.2 is a host-based intrusion prevention system designed to protect system resources and applications. It works to intercept system calls prior to their execution and network traffic prior to their processing. If the HIP Agent determines that a call or packet is symptomatic of malicious code, the call or packet can be blocked and/or an audit log created; if it determines that a call or packet is safe, it is allowed.

The HIP 6.0.2 Windows Agent (hereafter referred to as Agent) provides a protection layer that identifies and prevents malicious attempts to compromise a host. Agent software is installed on the host to be protected. Agents are operating system specific; only the Windows Agent is included in this evaluation.

In addition to the Agent, the TOE includes ePolicy Orchestrator (ePO) version 3.6.1 (Patch 1). ePO distributes and manages agents that reside on client systems. By using ePO you can manage a large enterprise network. A centralized but distributed architecture allows the Agent software to be centrally managed and yet decrease network traffic required to manage clients. ePO provides the management interface and functionality for the administrators of the TOE. It also provides centralized audit collection and review functionality.

1 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifier

Evaluation Identifiers for McAfee HIP and ePolicy Orchestrator system	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	McAfee HIP 6.0.2 and ePolicy Orchestrator 3.6.1 patch 1
Protection Profile	Intrusion Detection System System Protection Profile, Version 1.6, dated April 4, 2006
Security Target	McAfee Host Intrusion Prevention (HIP) v6.0.2 and ePolicy Orchestrator (EPO) v3.6.1 (Patch 1) Security Target, dated May 2007
Evaluation Technical Report	Evaluation Technical Report for McAfee HIP 6.0.2 and ePolicy Orchestrator 3.6.1 patch 1
Conformance Result	Part 2 conformant and EAL3 Part 3 conformant
Version of CC	CC Version 2.3 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on November 26, 2006
Version of CEM	CEM Version 2.3 and all applicable NIAP and International Interpretations effective on November 26, 2006
Sponsor	McAfee Inc.
Developer	McAfee Inc.
Evaluator(s)	**COACT Incorporated** Brian Pleffner Tony Busciglio Ching Lee Ryan Kane Brooks Leitch Pascal Patin
Validator(s)	**NIAP CCEVS,** Jerome F. Myers, David M. Dignan

1.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3

I-0426 – Content of PP Claims Rationale
I-0427 – Identification of Standards

International Interpretations

None

2 Security Policy

The TOE is the McAfee HIP and ePolicy Orchestrator that consists of a set of software components executed on Windows platforms. The TOE is comprised of two parts: the McAfee HIP agent and the ePolicy Orchestrator. McAfee HIP and ePolicy Orchestrator collectively is a Host Intrusion Protection tool and management tool intended for use in networked environments.

2.1 System Protection

The Agents are host based intrusion prevention systems designed to protect system resources and applications from attacks. The Agents accomplish this by intercepting operating system calls and comparing them to signatures symptomatic of known attacks and behavioral rules. The Agents also inspect network traffic by comparing packets to signatures symptomatic of known attacks. If a potential security violation is detected, the system call or network traffic may be allowed to proceed or be blocked. An audit event may also be generated.

2.2 Audit

The TOE generates audit records upon detection of a potential security violation or system configuration events. The audit records can be viewed by an authorized user. The TOE audit functionality includes the ability to configure what auditable events actually generate audit records.

2.3 Identification and Authentication

The TOE requires users to identify and authenticate themselves before accessing the TOE software or before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that defines the functionality the user is allowed to perform.

2.4 Management

The TOE's Management Security Function provides administrator functionality that enables a human user to configure and manage TOE components. Configuration functionality includes enabling a user to modify TSF Data used by the TOE's Security Functional Policies (SFPs). Management functionality includes invocation of TOE functions that effect security functions and security function behavior.

2.5 Security Function Strength of Function Claim

The claimed strength of function is SOF-basic. The Identification and Authentication Security function is a probabilistic function in the password mechanism. SOF-basic is appropriate for the intended use of the TOE in environments with threat agents with low attack potential.

2.6 Protection Profile Claim

This Security Target claims conformance to the Intrusion Detection System System Protection Profile, Version 1.6, dated April 4, 2006.

3 Assumptions

The specific conditions listed in the following subsections are assumed to be met by the environment and operating conditions of the system. The assumptions are ordered into three groups. They are personnel assumptions, physical assumptions, and IT environment assumptions.

A) Personnel assumptions describe characteristics of personnel who are relevant to the system.

B) Physical environment assumptions describe characteristics of the non-IT environment that the system is deployed in.

C) IT environment assumptions describe the technology environment within which the TOE is operating.

3.1 Physical Assumptions

The results of the evaluation rely upon the following assumptions regarding the physical environment.

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.2 IT Environment Assumptions

The results of the evaluation rely upon the following assumptions regarding the IT Environment.

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

3.3 Personnel Assumptions

The results of the evaluation rely upon the following assumptions regarding personnel relevant to the system.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

3.4 Threats

The following threats are addressed by the TOE and IT environment, respectively.

Threats Addressed by the TOE

The TOE addresses the following threats:

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

Threats Addressed by the IT environment

The IT environment addresses the following threats:

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

4 Clarification of Scope

The TOE is the McAfee HIP and ePolicy Orchestrator that consists of a set of software components executed on Windows platforms. The TOE is comprised of two parts: the McAfee HIP agent and the ePolicy Orchestrator. The evaluation does not make any statements about the adequacy or effectiveness of the McAfee HIP and ePolicy Orchestrator for its advertised usage in application firewalls, custom signatures and policies, importing configurations, and Linux and Solaris agents.

The underlying hardware and operating systems are not part of the TOE evaluation and the TOE relies upon their correct functionality to protect the TOE.

5 Architecture Information

The TOE consists of two software applications that execute on two different hardware platforms. These two software applications provide identification and authentication, audit, system protection, and management. The TOE is divided into two primary components, the ePolicy Orchestrator and HIP Agent.

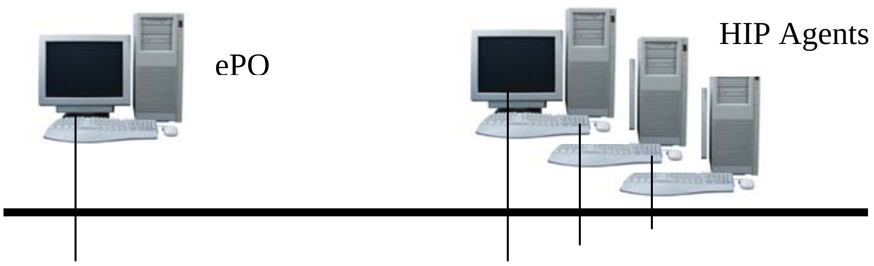

Figure 1 - TOE Components

5.1 Evaluated Configuration

Table 2 - Evaluated Configuration

Component	Version	Quantity
McAfee ePolicy Orchestrator	3.6.1 patch 1	1
McAfee HIP	6.0.2	1 or more

The following table summarizes the minimum hardware and software requirements for each of the TOE components.

Table 3 - Minimum Hardware and Software Requirements for the ePO Server

Hardware and Network Environment Requirements	
Free disk space	500MB
Processor	Intel Pentium II-class or higher; 450MHz or higher
Memory	512mb RAM
Monitor	1024 x 768; 256 color, VGA monitor
NIC	Network Interface Card with 100mb capacity
File system	NTFS partition
IP Address	Static IP Address

Software Components and Requirements of the Environment	
DBMS (one of the following is required)	Microsoft SQL Server 2000 Standard with SP 3
	Microsoft SQL Server 2000 Enterprise with SP 3
	Microsoft SQL Server 7 Standard with SP 3 or 4
	Microsoft SQL Server 7 Enterprise with SP 3 or 4
Browser	Microsoft Internet Explorer v6.0
Domain Controller	The server must have a trust relationship with the Primary Domain Controller (PDC) on the network.
JAVA Runtime Environment	JRE 1.4.2_02
JDBC Driver	jTDS driver 1.2
Crystal Reports	8.0/8.5
Agent-Server Communication	Apache 2.0.54
Web Server	Apache 2.0.54
Application Server	Tomcat 4.1.30
TLS	PGP SDK 3.5.3

The following configuration options must be used in the evaluated configuration:

A) All user accounts defined in ePO must specify ePO authentication (rather than NT authentication)

5.2 Functionality Excluded from the Evaluation

- Firewall functionality (some government users require firewall functionality to be disabled unless it has been evaluated against one of the firewall PPs at EAL4 or Medium Robustness). Application Blocking functionality is associated with the firewall functionality and is also excluded.
- Custom signatures and policies.
- Importing configurations.
- HIP Solaris Agents.
- HIP Linux Agents.

6 Product Delivery

The TOE delivery is via download from a secure FTP site operated by McAfee.

The download site has available the correct version of software clearly labeled:

McAfee HIP 6.0.2
ePolicy Orchestrator 3.6.1 patch 1

The download site also contains the following documents for download (all were part of the evaluation):

ePolicy Orchestrator (EPO) Deploy and manage security products and network systems version 3.6 Installation Guide

McAfee Host Intrusion Prevention (HIP) v6.0 for use with ePolicy Orchestrator (EPO) v3.6 Installation/Configuration Guide
McAfee® Host Intrusion Prevention version 6.0 Product Guide
ePolicy Orchestrator Deploy and manage security products and network systems version 3.6 Product Guide
Host Intrusion Prevention version 6.0 Quick Reference Card
Intrusion Detection and Intrusion Prevention Software Managed by ePolicy Orchestrator 3.6.1 (Patch 1)
ePolicy Orchestrator version 3.6 Quick Reference Card
Troubleshooting with Log Files Guide ePolicy Orchestrator® version 3.6
ePolicy Orchestrator Walkthrough Guide
ePolicy Orchestrator Reporting Guide

7 IT Product Testing

Testing was performed on February 21 through February 27 at the COACT Laboratory in Columbia, MD. Two COACT employees performed the tests.

7.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of a four test PCs, hub, two McAfee HIP Agents, and the ePolicy Orchestrator, and attack software.

Figure 2 - Test Configuration/Setup

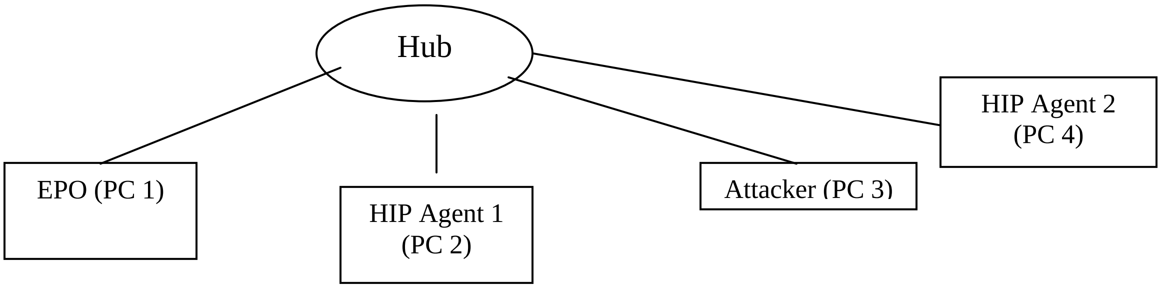

Table 4 - Test Configuration

Component	Description
ePO Server Computer	EPolicy Orchestrator 3.6.1 patch 1 Pentium 4, 1.70 GHz 512 MB RAM Microsoft Windows 2000 Server Service Pack 4
Agent PC 1	HIP 6.0.2 agent Pentium 4, 1.70 GHz 384 MB RAM Microsoft Windows XP Professional Version 2002

	Service Pack 2 NmapGUI v.0.2 NeWT Security Scanner v.2.2.1 Wireshark v.99.4
Agent PC 2	HIP 6.0.2 agent Pentium 4, 3.20 GHz 2 GB RAM Microsoft Windows XP Professional Version 2002 Service Pack 2 NmapGUI v.0.2 NeWT Security Scanner v.2.2.1 Wireshark v.99.4
Attack PC	Pentium 4, 1.60 GHz 228 MB RAM Microsoft Windows 2000 Server Service Pack 4 NmapGUI v.0.2 The Dude v.2.0 Wireshark v.99.4 Tenable Nessus Security Scanner version 3.0.3 Tiger Suite v.4.5 Cain & Abel v.3.9
Hub	3Com 10Base-T Hub

7.2 Functional Test Results

The vendor chose not to use the original test suite from the development of the TOE. The vendor instead generated a customized test suite that focused on testing the specific security requirements in the Security Target. The evaluation team executed the entire developer test suite except for one test case. All tests were performed satisfactorily and the results were as expected. The TOE passed all tests. The procedures followed to execute these tests and detailed results are presented in the developer and CCTL proprietary report, McAfee HIP Functional Test Report F3-0507-006*,* dated 5 March 2007.

7.3 Evaluator Independent Testing

The evaluation team performed an analysis of all of the developer tests to assess the level of developer testing corresponding to each of the TSFIs. The following tests were performed during independent functional testing:

To ensure that the ePO server records authentication failures.
To ensure that creating or modifying Trust Application Rules are recorded in the audit log.
ePO Policies Details Pane Test
Adding User to Exception Rules
Viewing IPS Events Summary
Adding User to Exception Rules
Adding Parameter to Exception Rules
Viewing IPS Events Properties Tab
Adding User to Exception Rules
Using Search IPS Exception Rules

The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests. All tests were performed satisfactorily and the results were as expected. The TOE passed all tests.

7.4 Evaluator Penetration Tests

The evaluators examined the developer's vulnerability analysis. The developer concluded that there are currently no known obvious vulnerabilities with the TOE. The developer checked numerous public databases including http://www.cert.org, http://www.securityfocus.com, http://nvd.nist.gov/, http://www.osvdb.org/, and http://archives.neohapsis.com/ with no obvious vulnerabilities existing for the TOE.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if any obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities.

As a result of the evaluator's examination of the developer's vulnerability analysis and the independent search for obvious TOE vulnerabilities, the evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the vulnerabilities. The scope of evaluator analysis and testing included potential obvious vulnerabilities in the IT Environment that would be introduced as a result of the presence of the TOE. The following Penetration tests were performed by the evaluator:

1. Overwhelming the management console with ICMP (ping), HTTP, and FTP requests simultaneously may result in the TOE granting unauthorized access to the administrative options.
2. Although trusted channels are provided the TOE may not use them when communicating between distributed TOE components allowing inter-TOE communication to be compromised.
3. Disable the ePO by sending ill-formed remote requests.
4. It may be possible to circumvent the TOE enforced Policies by changing and pushing a new policy while the HIP agent is being accessed.
5. It may be possible to compromise the TOE by spoofing the IP Address of an authorized agent and attempting to perform unauthorized actions or pull unauthorized information from the ePO
6. It may be possible to cause the TOE to use unprotected communications for inter-TOE traffic by corrupting the .dll that provides the functionality.
7. It may be possible for a non-trusted user to access the .dll that provides communication protection and corrupt/disrupt inter-TOE communications.
8. It may possible to gain unauthorized access to the database housing the TOE audit records by accessing the DB through in unconventional ways.

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, COACT document F3-0507-005 McAfee HIP Penetration Test Report, dated 05 March 2007.

7.5 Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

8 RESULTS OF THE EVALUATION

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 3 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the COACT document F3-0507-004, for the Evaluation Technical Report for McAfee HIP 6.0.2 and ePolicy Orchestrator 3.6.1 patch 1, dated 08 May 2007 contains the verdicts of "PASS" for all the work units.

The evaluation determined that the product meets the requirements for EAL 3. The details of the evaluation are recorded in the, Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10. VALIDATOR COMMENTS

The Validators found that the evidence reviewed prior and during the Final Validation Oversight Review (VOR) supported the determination that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validators agree that the CCTL presented appropriate rationales to support the evaluation results presented in Evaluation Technical Report for the" McAfee HIP 6.0.2 and Epolicy Orchestrator 3.6.1 patch 1. The Validators conclude that the evaluation and Pass result for the ST and TOE are complete and correct.

11. Security Target

The McAfee Host Intrusion Prevention (HIP) v6.0.2 and ePolicy Orchestrator (EPO) v3.6.1 (Patch 1) Security Target, dated May 2007, is incorporated here by reference.

12. List of Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
HIP	Host Intrusion Prevention
IDS	Intrusion Detection System
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute for Standards Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control

TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VOR	Validation Oversight Review

13. Bibliography

The following list of standards was used in this evaluation:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.3, dated August 2005
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.3, dated August 2005
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.3, dated August 2005
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.3, dated August 2005
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.3, dated August 2005
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000