

National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



Validation Report

for the

Cisco Catalyst 9200L and 9400 Series Switches running IOS-XE 16.9, Version 1.0

Report Number: CCEVS-VR-VID10972-2019

Dated: 07/24/19

Version: 1.0

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 6940

Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell, Senior

John Butterworth, Lead

Jenn Dotson

Claire Olin

Linda Morrison

Patrick Mallett

The MITRE Corporation

Common Criteria Testing Laboratory

Danielle F Canoles

Kenneth Lasoski

Acumen Security, LLC

Table of Contents

1	Executive Summary	4
2	Identification	5
3	Architectural Information	6
4	Security Policy	7
5	Assumptions, Threats & Clarification of Scope	10
5.1	Assumptions	10
5.2	Threats.....	11
5.3	Clarification of Scope	13
6	Documentation	14
7	TOE Evaluated Configuration	15
7.1	Evaluated Configuration.....	15
7.2	Physical Scope of the TOE	15
7.3	Excluded Functionality	15
8	IT Product Testing	16
8.1	Developer Testing	16
8.2	Evaluation Team Independent Testing.....	16
9	Results of the Evaluation	17
9.1	Evaluation of Security Target	17
9.2	Evaluation of Development Documentation	17
9.3	Evaluation of Guidance Documents	17
9.4	Evaluation of Life Cycle Support Activities	17
9.5	Evaluation of Test Documentation and the Test Activity	18
9.6	Vulnerability Assessment Activity	18
9.7	Summary of Evaluation Results	18
10	Validator Comments & Recommendations	19
11	Annexes	20
12	Security Target	21
13	Glossary	22
14	Bibliography	23

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Catalyst 9200L and 9400 Series Switches running IOS-XE 16.9 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in July 2019. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for NDcPP 2.0e.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the NDcPP 2.0e. This Validation Report applies only to the specific version of the TOE as evaluated. 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 provided.

A validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation demonstrated that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance claims are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring 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's Product Compliant List.

The following table provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cisco Catalyst 9200L and 9400 Series Switches running IOS-XE 16.9
Protection Profile	NDcPP 2.0e
Security Target	Cisco Catalyst 9200L and 9400 Series Switches running IOS-XE 16.9 Security Target, Version 1.0, 11 June 2019
Evaluation Technical Report	Cisco Catalyst 9200L and 9400 Series Switches running IOS-XE 16.9 ETR, Version 1.1, June 2019
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Paul Bicknell Senior Validator John Butterworth Lead Validator Jenn Dotson Lisa Mitchell Linda Morrison Clare Olin Patrick Mallett The MITRE Corporation

3 Architectural Information

The TOE is a hardware and software solution that makes up the switch models as follows: Catalyst 9200L and 9400 Series Switches running Cisco IOS-XE 16.9. The network, on which they reside, is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Catalyst 9200L and 9400 Series Switches Common Criteria Operational User Guidance and Preparative Procedures document and are downloadable from the <http://cisco.com> web site. The TOE is comprised of the following physical specifications as described in Table 5 below. The hardware, size and the interfaces are based on the number of ports on a particular model.

4 Security Policy

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

Security Audit

The Cisco Catalyst 9200L and 9400 Series Switches provides extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity that triggered the event and the outcome of the event.

The TOE is configured to transmit the audit messages to an external syslog server. Communication with the syslog server is protected by using IPsec and the TOE can determine when communication with the syslog server fails. If that should occur, the TOE can be configured to block new permit actions.

The audit logs can be viewed on the TOE using the appropriate IOS commands. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to clear (delete) audit data stored locally on the TOE.

Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates (Operation Environment – ARM A53 (9200L) and Intel Xeon D (9400) processor).

The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5 as identified in the table below. The IOS software calls the IOS Common Cryptographic Module (IC2M) Rel5 (Firmware Version: Rel 5) that has been validated for conformance to the requirements of FIPS 140-2 Level 1

The TOE provides cryptography in support of VPN connections that includes remote administrative management via SSHv2 and IPsec to secure the transmission of audit records to the remote syslog server. In addition, IPsec is used to secure the session between the TOE and the authentication servers.

Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication. The IKE phase authentication for the IPsec communication channel between the TOE and

authentication server and between the TOE and syslog server is considered part of the Identification and Authentication security functionality of the TOE.

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSHv2 interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE supports use of a RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

The TOE also provides an automatic lockout when a user attempts to authenticate and enters invalid information. When the threshold for a defined number of authentication attempts fail has exceeded the configured allowable attempts, the user is locked out until an authorized administrator can enable the user account.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections.

Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection.

The TOE supports two separate administrator roles: non-privileged administrator and privileged administrator. Only the privileged administrator can perform the above security relevant management functions. The privileged administrator is the Authorized Administrator of the TOE who has the ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE as described in this document.

Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, Cisco IOS-XE is not a general-purpose operating system and access to Cisco IOS-XE memory space is restricted to only Cisco IOS-XE functions.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. The TOE provides the Authorized Administrators the capability to update the TOE's clock manually to maintain a reliable timestamp.

Finally, the TOE performs testing to verify correct operation of the TOE itself and that of the cryptographic module.

TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the remote authentication servers.

The TOE can also establish trusted paths of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog server.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g.

Assumption	Assumption Definition
	cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

Threat	Threat Definition
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker’s credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.

Threat	Threat Definition
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the NDcPP 2.0e.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cisco Catalyst 9200L and 9400 Series Switches running IOS-XE 16.9 Security Target, v1.0
- Cisco Catalyst 9200L and 9400 Series Switches running IOS-XE 16.9 Common Criteria Operational User Guidance And Preparative Procedures, v1.0

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE consists of one or more physical devices as described below and includes the Cisco IOS-XE 16.9 software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The switch configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

In addition, if the Catalyst 9200L and 9400 Series Switches is to be remotely administered, then the management workstation must be connected to an internal network, SSHv2 is used to securely connect to the switch. A syslog server is used to store audit records, where IPsec is used to secure the transmission of the records. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

7.2 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the switch models as follows: the Catalyst 9200L and 9400 Series running Cisco IOS-XE 16.9. The switch chassis provides power, cooling and backplane for the Network Module, Supervisor Engine, line cards and service modules. The network, on which they reside, is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Cisco Catalyst 9200L and 9400 Series Switches Common Criteria Operational User Guidance and Preparative Procedures document and are downloadable from the <http://cisco.com> web site. The TOE is comprised of the following physical specifications as described in the ST. The hardware, size and the interfaces are based on the number of ports on a particular model.

7.3 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 1 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.

This service can be disabled by configuration settings as described in the Guidance documents (AGD). The exclusion of this functionality does not affect the compliance to the collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Cisco Catalyst 9200L and 9400 Series Switches, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDcPP 2.0e. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Cisco Catalyst 9200L and 9400 Series Switches to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Catalyst 9200L and 9400 Series Switches that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the NDcPP 2.0e.

9.2 Evaluation of Development Documentation

The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally the evaluator performed the Assurance Activities specified in the NDcPP 2.0e related to the examination of the information contained in the TOE Summary Specification.

9.3 Evaluation of Guidance Documents

The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the NDcPP 2.0e related to the examination of the information contained in the operational guidance documents.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team found that the TOE was identified and appropriately labeled.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP 2.0e and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

9.6 Vulnerability Assessment Activity

The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

10 Validator Comments & Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

Consumers employing the devices must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Annexes

Not applicable.

12 Security Target

Cisco Catalyst 9200L and 9400 Series Switches running IOS-XE 16.9 Security Target, Version 1.0, 11 June 2019

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.