National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



TM

Validation Report
for the
MPIC2 v4.3

Report Number: CCEVS-VR-VID11721-2026
Dated: 29 October 2026
Version: 1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson

Sheldon Durrant

Lisa Mitchell

Jaemond Reyes

Lori Sarem

Joe Walton

The MITRE Corporation

Common Criteria Testing Laboratory

Kevin Steiner

Raj Mendon

Lightship Security USA, Inc.

Table of Contents

1. Executive Summary 1
2. Identification 2
3. Architectural Information 4
   3.1. TOE Evaluated Configuration 4
   3.2. Physical Boundary 4
   3.3. Required Non-TOE Hardware, Software, and Firmware 5
4. Security Policy 6
   4.1. Security Audit 6
   4.2. Cryptographic Support 6
   4.3. Identification and Authentication 6
   4.4. Security Management 6
   4.5. Protection of the TSF 6
   4.6. TOE Access 6
   4.7. Trusted Path/Channels 6
5. Assumptions & Clarification of Scope 7
   5.1. Assumptions 7
   5.2. Clarification of Scope 7
6. Documentation 8
7. IT Product Testing 9
   7.1. Developer Testing 9
   7.2. Evaluation Team Independent Testing 9
   7.3. Evaluated Configuration 9
8. Results of the Evaluation 11
   8.1. Evaluation of Security Target (ASE) 11
   8.2. Evaluation of Development Documentation (ADV) 11
   8.3. Evaluation of Guidance Documents (AGD) 11
   8.4. Evaluation of Life Cycle Support Activities (ALC) 12
   8.5. Evaluation of Test Documentation and the Test Activity (ATE) 12
   8.6. Vulnerability Assessment Activity (VAN) 12
   8.7. Summary of Evaluation Results 13
9. Validator Comments 14

10. Annexes 15
11. Security Target 16
12. Glossary 17
13. Acronym List 18
14. Bibliography 19

List of Tables

Table 1: Evaluation Identifiers 2
Table 2: TOE Models 4
Table 3: Tools Used for Testing 10

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of MPIC2 v4.3 provided by CAE Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in October 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the:

- *Collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023 (NDcPP30e) and
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 (SSH10).

The TOE is MPIC2 v4.3. The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the *Common Methodology for IT Security Evaluation* (Version 3.1, Rev 5) for conformance to the *Common Criteria for IT Security Evaluation* (Version 3.1, Rev 5). This VR 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *CAE MPIC2 v4.3 Security Target*, Version 1.11, October 2026, and analysis performed by the Validation team.

2. 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) in accordance with National Voluntary Laboratory Accreditation 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 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 Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product	CAE MPIC2 v4.3
Sponsor and Developer	CAE Inc. 8585 Cote-de-Liesse, Montreal, Quebec, Canada, H4T 1G6
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 5, April 2017.
CEM	*Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	*collaborative Protection Profile for Network Devices*, Version: 3.0e, Date: 06-December-2023 *Functional Package for Secure Shell (SSH)*, Version: 1.0, Date 13-May-2021
ST	*CAE MPIC2 v4.3 Security Target*, Version 1.11, October 2026
Evaluation Technical Report	*CAE MPIC2 v4.3 Evaluation Technical Report*, Version 1.2, October 2026
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Raj Mendon
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Jaemond Reyes, Lori Sarem, Joe Walton

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target (ST)

The CAE MPIC2 is a standalone physical Network Device, used to transmit data from the hardware panels to a software-based flight simulation, processed by one or more Daughter Boards (DB). The simulation data is processed by the DB's and then feedback is transmitted back to the hardware panels via the MPIC2. It comes in a range of form factors (see Table 2). The different form factors can be installed in combination or independently to Network data. All form factors provide a basic set of security functions such as, a secure remote management path, identification and authentication services to trusted administrators, and secure auditing of administrator actions. The form factors are not security relevant and the claimed SFRs are supported across all TOE models.

The MPIC2-PCIe form factor differs as it is designed to support additional sensor and communication technologies (Can-Bus, A429, WXR). The MPIC2-EMB-CPU differs as it is designed to be embedded and not mounted into systems. The MPIC2-EMB-CPU-POE is also designed to be embedded and further differs as it supports Power-Over-Ethernet. The MPIC2-ILAC differs as its main function is to supply variable AC voltage to the cockpit integral lighting.

3.1. TOE Evaluated Configuration

The TOE is a network device that transmits data between the hardware panels to a software-based flight simulator. The TOE interfaces are as follows:

CLI. CLI via Serial and CLI via remote SSH connection

Logs. The TOE uses a Syslog server.

NTP. The TOE synchronizes time via NTP.

Instrument. The TOE transmits simulation data between the software-based simulator and the hardware panels.

Simulation. The TOE transmits simulation data between the software-based simulator and the hardware panels.

3.2. Physical Boundary

The physical boundary of the TOE includes all software and hardware shown in Table 2. The TOE is delivered via commercial courier.

Table 2: TOE Models

Type/Model	CPU	Part Number	Software	Differences
MPIC2	i.MX8 Plus Dual Core CPU Cortex A53 & Cortex M7 with CAAM (uSD socket)	MA594260.61.2.268	cae-mx6qmpic-4.3.28.0 MPICLinuxDistributionX R 4.3	Form Factor
	i.MX8 Plus Dual Core CPU Cortex A53 & Cortex M7	MA594260.62.2.268		

Type/Model	CPU	Part Number	Software	Differences
	with CAAM (uSD socket and eMMC)		Linux Yocto Project 'Scarthgap' (v5.0)	
MPIC2-PCIe	i.MX8 Plus Dual Core CPU Cortex A53 & Cortex M7 with CAAM (uSD socket)	MA594266.61.2.268		
	i.MX8 Plus Dual Core CPU Cortex A53 & Cortex M7 with CAAM (uSD socket and eMMC)	MA594266.62.2.268		
MPIC2-EMB-CPU	i.MX8 Plus Dual Core CPU Cortex A53 & Cortex M7 with CAAM (uSD socket)	MA610150.61.2.268		
	i.MX8 Plus Dual Core CPU Cortex A53 & Cortex M7 with CAAM (uSD socket and eMMC)	MA610150.62.2.268		
MPIC2-EMB-CPU-POE	i.MX8 Plus Dual Core CPU Cortex A53 & Cortex M7 with CAAM (uSD socket)	MA610102.61.2.268		
	i.MX8 Plus Dual Core CPU Cortex A53 & Cortex M7 with CAAM (uSD socket and eMMC)	MA610102.62.2.268		
MPIC2-ILAC	i.MX8 Plus Dual Core CPU Cortex A53 & Cortex M7 with CAAM (uSD socket)	MA610166.61.2.268		
	i.MX8 Plus Dual Core CPU Cortex A53 & Cortex M7 with CAAM (uSD socket and eMMC)	MA610166.62.2.268		

Note: The Cortex M7 is not used by the TOE to support any of the cryptographic functionality and is considered outside the cryptographic boundary and is in the operational environment.

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

- **Audit Server.** The TOE sends audit events to syslog server.
- **NTP Server.** The TOE synchronizes time via NTP.
- **Instrument.** The TOE transmits simulation data between the software-based simulator and the hardware panels.
- **Simulator.** The TOE transmits simulation data between the software-based simulator and the hardware panels.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Security Audit

The TOE generates audit records of user and administrator actions. The TOE includes the user identity in audit events resulting from actions of identified users. The Security Administrator can configure the TOE to send logs in real-time to a syslog server via SSH.

4.2. Cryptographic Support

The TOE implements a cryptographic module. The cryptographic module has the ability to generate and destroy cryptographic keys. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are provided in Table 12 of the ST.

4.3. Identification and Authentication

The TOE ensures that all users must be authenticated before accessing its functions and data. When a user account has sequentially failed authentication the configured number of times, the account will be locked for a Security Administrator defined time period.

4.4. Security Management

The TOE enables secure management of its security functions, including:

- Administrator authentication with passwords
- Configurable password policies
- Role Based Access Control
- Access banners
- Management of critical security functions and data
- Protection of cryptographic keys and passwords

4.5. Protection of the TSF

The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions. The TOE performs diagnostic self-tests and cryptographic module self-tests during start-up. Administrators are provided with the ability to manually update the TOE. The TOE makes use of secure NTP to maintain date and time.

4.6. TOE Access

The TOE can be accessed directly via serial connection or remotely via SSH connection. The TOE provides the ability to configure termination behavior of inactive local and remote sessions. Administrators can configure an advisory notice displayed prior to login.

4.7. Trusted Path/Channels

The TOE protects the integrity and confidentiality of communications as discussed in Section 3.1 above, and using cryptographic algorithms as described in Table 12 of the ST.

5. Assumptions & Clarification of Scope

5.1. Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e)
- *Functional Package for SSH*, Version 1.0, 13 May 2021 (SSH10)

That information has not been reproduced here and the NDcPP30e/SSH10 should be consulted if there is interest in that material.

5.2. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP30e/SSH10 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 assurance activities specified in the NDcPP30e/SSH10 and performed by the Evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide identified in Section 6, additional customer documentation for the specific Network Device models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP30e/SSH10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6. Documentation

The following guidance document is provided with the TOE upon delivery in accordance with the PP:

- *CAE MPIC2 v4.3 Common Criteria Guide,* Version 1.4, October 2026

Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and, therefore, should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation team. It is derived from information contained in the proprietary *CAE MPIC2 v4.3 NDcPPv3.0e Detailed Test Report*, Version 1.2, October 2026 (DTR), as summarized in the *CAE MPIC2 v4.3 Assurance Activity Report,* Version 1.2, October 2026 (AAR).

7.1. Developer Testing

No evidence of developer testing is required in the Security Assurance Requirements (SARs) or Evaluation Activities.

7.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from May 2026 until August 2026. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the ST.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the NDcPP30e/SSH10 test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the Evaluation team verified that each test passed.

7.3. Evaluated Configuration

The TOE testing environment components are identified in Figure 1 and Table 3 below.

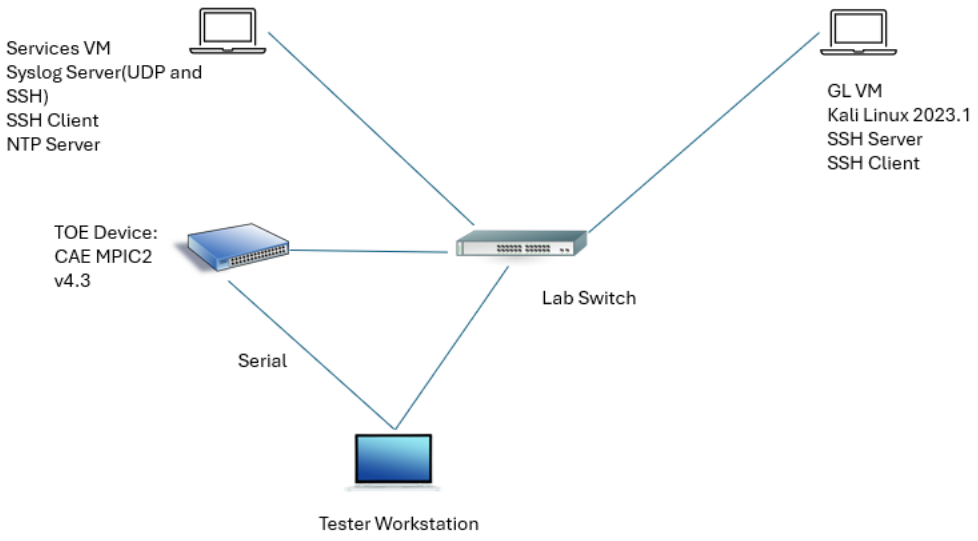


Figure 1: Testing Environment Overview

Table 3: Tools Used for Testing

Tool name	Version	Description
Lightship Greenlight	3.0.35	Used to provide automated support for SSH and NTP protocol testing.
Wireshark	4.0.8 (Linux) & 4.6.7 (Windows)	Used for packet capture and analysis
Tcpdump	4.9.3 & 4.99.1	Used for packet capture and analysis
OpenSSH	8.8p1	Used for general purpose SSH CLI access, also used for remote logging.
Sylog-ng	3.19.1	Syslog server

8. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary DTR and ETR documents. The reader of this document can assume that all assurance 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 5 and CEM version 3.1 rev 5. The evaluation determined the MPIC2 v4.3 TOE to be Part 2 extended, and to meet the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in NDcPP30e/SSH10.

8.1. Evaluation of Security Target (ASE)

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 MPIC2 v4.3 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team 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.

8.2. Evaluation of Development Documentation (ADV)

The Evaluation team applied each ADV CEM work unit. 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 ST and Guidance document. Additionally, the Evaluation team performed the assurance activities specified in the NDcPP30e/SSH10 related to the examination of the information contained in the TSS.

The Validation 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.

8.3. Evaluation of Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. 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 guide was assessed during the design and testing phases of the evaluation to ensure it was complete.

The Validation team 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.

8.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team 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.

8.5. Evaluation of Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the NDcPP30e/SSH10 and recorded the results in a Test Report, summarized in the ETR and AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence was provided by the Evaluation team to show that the evaluation activities addressed the test activities in the NDcPP30e/SSH10, and that the conclusion reached by the Evaluation team was justified.

8.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is documented in the *CAE MPIC2 v4.3 Vulnerability Assessment*, Version 1.1, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on October 23, 2026 did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html
- US-CERT: http://www.kb.cert.org/vuls/html/search
- CVE details: https://www.cvedetails.com/vulnerability-search.php
- CISA KEV: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

The Evaluation team performed a search using the following keywords:

- CAE
- CAE MPIC2
- MPIC2
- MPIC2-PCIe
- MPIC2-EMB-CPU
- MPIC2-EMB-CPU-POE
- MPIC2-ILAC

- i.MX8 Plus
- Cortex A53
- Cortex M7
- Iptables
- Linux kernel
- Openssh
- Openssl
- ntp
- auditd
- python
- Linux Yocto Project 'Scarthgap' (v5.0)

The Validation team 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.

8.7. 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.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM, performed the Assurance Activities in the NDcPP30e/SSH10, and correctly verified that the product meets the claims in the ST.

9. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 6 of this VR. No other versions of the TOE and software, either earlier or later, were evaluated.

The evaluated functionality is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionalities provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

Per NIAP/CCEVS Publication #6, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

10. Annexes

Not applicable.

11. Security Target

CAE MPIC v4.3 Security Target, Version 1.11, October 2026

12. GLOSSARY

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

14. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *Collaborative Protection Profile for Network Devices,* Version: 3.0e, 6 December 2023
6. *Functional Package for Secure Shell (SSH),* Version: 1.0, 13 May 2021
7. *CAE MPIC2 v4.3 Security Target,* Version 1.11, October 2026 (ST)
8. *CAE MPIC2 v4.3 Common Criteria Guide,* Version 1.4, October 2026 (AGD)
9. *CAE MPIC2 v4.3 Assurance Activity Report,* Version 1.2, October 2026 (AAR)
10. *CAE MPIC2 v4.3 Vulnerability Assessment,* Version 1.1, October 2026 (AVA)
11. *CAE MPIC2 v4.3 Evaluation Technical Report*, Version 1.2, October 2026 (ETR)
12. *CAE MPIC2 v4.3 NDcPPv3.0e Detailed Test Report,* Version 1.2, October 2026 (DTR)
13. *CAE MPIC2 v4.3 Test Evidence,* Version 1.1, October 2026