# National Information Assurance Partnership
# Common Criteria Evaluation and Validation Scheme


TM

# Validation Report
# for the
# CAE MPIC v3.5

**Report Number:** CCEVS-VR-VID11575-2025
**Dated:** June 5, 2025
**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**

Lisa Mitchell

Clare Parran

Chris Thorpe

**The MITRE Corporation**

**Common Criteria Testing Laboratory**

Kevin Steiner

Joon Sim

**Lightship Security USA, Inc.**

# Table of Contents

## List of Tables

# 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 Threats in Section 5, Clarification of Scope in Section 6 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation Team of the evaluation of MPIC v3.5 provided by CAE Inc. It presents the evaluation results, their justifications, and the conformance results. This 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. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in June 2025. 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 and *Functional Package for Secure Shell (SSH)*, Version: 1.0.

The TOE is CAE MPIC v3.5. 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.

# 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 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 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.

**Error! Reference source not found.** 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 MPIC v3.5 |
| Sponsor and Developer | CAE Inc.<br>8585 Cote-de-Liesse, Montreal, Quebec, Canada, H4T 1G6 |
| CCTL | Lightship Security USA, Inc.<br>3600 O'Donnell St., Suite 2<br>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 [CPP_ND_V3.0E]<br>*Functional Package for Secure Shell (SSH)*, Version: 1.0, Date 13-May-2021 [PKG_SSH_V1.0] |
| ST | *CAE MPIC v3.5 Security Target*, v1.11, May 2025 |
| Evaluation Technical Report | *CAE MPIC v3.5 Evaluation Technical Report*, v1.5, May 2025 |
| Conformance Result | CC Part 2 extended, CC Part 3 conformant |
| Evaluation Personnel | Joon Sim |
| CCEVS Validators | Lisa Mitchell, Clare Parran, Chris Thorpe |

# 3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The CAE MPIC 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 MPIC. 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 MPIC-PCMIP form factor differs as it has a standard type slot for extensions compared to the custom interface on the MPIC. The MPIC-EMB differs as it is designed to be embedded and not mounted into systems. The MPIC-ILAC differs as its main function is to supply variable AC voltage to the cockpit integral lighting. The MPIC-SBC differs as its main function is to provide faster ethernet computing with a second ethernet port and a 48 pin daughterboard connector for demanding autopilot simulation.

## 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:

**a)** **CLI.** CLI via Serial and CLI via remote SSH connection

**b)** **Logs.** The TOE uses a Syslog server.

**c)** **NTP.** The TOE synchronizes time via NTP.

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

**e)** **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 **Error! Reference source not found.**.

The TOE is delivered via commercial courier.

**Table 2: TOE Models**

| Type/Model | CPU | Part Number | Software | Differences |
|---|---|---|---|---|
| MPIC | i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM | MA505400.61.2.268 | | Form Factor |

| Type/Model | CPU | Part Number | Software | Differences |
|---|---|---|---|---|
| MPIC-PCMIP | i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM | MA505402.61.2.268 | cae-mx6qmpic-3.5.10 MPICLinuxDistributionXR 3.5 | |
| MPIC-EMB | i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM | MA505404.61.2.268 | | |
| MPIC-EMB | i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM (quad-core) | MA505404.62.2.268 | | |
| MPIC-ILAC | i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM | MA563540.61.2.268 | | |
| MPIC-SBC | i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM (quad-core) | MA563510.61.2.268 | | |

### 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 shown in Table 4 of the ST.

## 4.3. Identification and Authentication

The TOE ensures that all users must be authenticated before accessing its functions and data.

## 4.4. Security Management

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

a) Administrator authentication with passwords

b) Configurable password policies

c) Role Based Access Control

d) Access banners

e) Management of critical security functions and data

f) 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.

## 4.6. TOE Access

TOE can be accessed directly via serial connection or remotely via SSH connection. 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.

## 4.7. Trusted Path/Channels

The TOE protects the integrity and confidentiality of communications as noted in the ST, and using cryptographic algorithms as claimed in the ST.

# 5. Assumptions

Only the Assumptions are reproduced below. For a complete set of Threats and Security Objectives met by the TOE, CPP_ND_V3.0E/PKG_SSH_V1.0 can be referenced.

**Table 3: Assumptions**

| Identifier | Description |
|---|---|
| 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 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 does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For vNDs, this assumption applies to the physical platform on which the VM runs. |
| 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 a computing platform for general purpose applications (unrelated to networking functionality).<br><br>If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform. |
| 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 and PP-Modules 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 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.<br><br>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification). |

| Identifier | Description |
|---|---|
| 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. |
| A.RESIDUAL_ INFORMATION | The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. |

# 6. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V3.0E/PKG_SSH_V1.0 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 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 in accordance with the evaluation activities specified in CPP_ND_V3.0E/PKG_SSH_V1.0 and performed by the Evaluation Team.
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- Apart from the Common Criteria Guide and the Getting Started Guide referenced in the Bibliography, additional customer documentation for the specific 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 CPP_ND_V3.0E/PKG_SSH_V1.0 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

# 7. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

*a)* *CAE MPIC v3.5 Common Criteria Guide*, Version 1.2, May 2025

*b)* *Getting Started with MPIC Developer's Guide*, TPD 20365 Rev9, 07 October 2024

All documentation delivered with the product is relevant to and within the scope of the TOE.

# 8. IT Product Testing

This section describes the testing efforts of the Evaluation Team. It is derived from information contained in *CAE MPIC v3.5 Assurance Activity Report,* Version 1.6, May 2025 provides an overview of testing and the prescribed evaluation activities.

## 8.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities.

## 8.2. Evaluation Team Independent Testing

The Evaluation Team conducted independent testing at Lightship Security USA in Baltimore, MD from October 2024 until May 2025. The Evaluation Team configured the TOE according to vendor installation instructions and as identified in the Security Target.

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 Protection Profile 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.

## 8.3. Evaluated Configuration

The TOE testing environment components are identified in Figure 1 and Table 4 below.

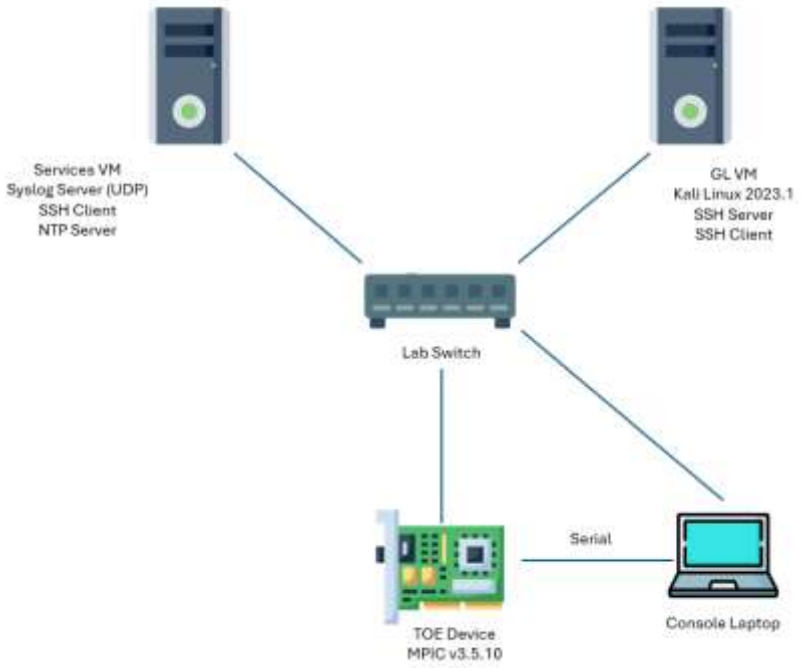

**Figure 1: Testing Environment Overview**

**Table 4: 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) & 3.6.16 (Windows) | Used for packet capture and analysis |
| tcpdump | 4.99.1 | Used for packet capture and analysis |
| OpenSSH | OpenSSH 8.8p1 | Used for general purpose SSH CLI access, also used for remote logging. |
| syslog-ng | 3.19.1 | Syslog server |

# 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 all 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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined MPIC v3.5 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in CPP_ND_V3.0E-SD/PKG_SSH_V.10.

## 9.1. 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 MPIC v3.5 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.

## 9.2. 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 documents. Additionally, the Evaluation Team performed the Evaluation Activities related to the examination of the information contained in the TSS.

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.

## 9.3. 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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were 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.

### 9.4. 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.

### 9.5. 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 Test Evaluation Activities and recorded the results in a Test Report, summarized in the AAR.

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.

### 9.6. Vulnerability Assessment Activity (VAN)

The Evaluation Team applied each AVA CEM work unit. The vulnerability analysis is in the *CAE MPIC v3.5 Vulnerability Assessment*, Version 1.6 report prepared by the Evaluation Team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on May 27, 2025, 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
- Tenable Network Security: https://www.tenable.com/cve
- Tipping Point Zero Day Initiative: https://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

The Evaluation Team performed a search using the following keywords:

- CAE MPIC
- CAE
- MPIC
- MPIC-PCMIP
- MPIC-EMB
- MPIC-ILAC
- MPIC-SBC
- ARM Cortex-A9
- i.MX6
- iptables 1.6.2
- Linux Kernel 4.9.67-fslc
- Openssh 7.8p1
- OpenSSL 1.0.2r
- ntp 4.2.8p12
- auditd 2.8.4
- Python 2.7.16

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.

### 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.

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 and performed the Evaluation Activities in CPP_ND_V3.0E-SD/PKG_SSH_V1.0, and correctly verified that the product meets the claims in the ST.

# 10. 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 7 of this VR. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. 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.

The functionality evaluated 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, specifically the functionality described in section 2.4.3 of the ST. Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

# 11. Annexes

Not applicable.

# 12. Security Target

*CAE MPIC v3.5 Security Target*, Version 1.11, May 2025

# 13. 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.

# 14. Acronym List

**Table 5: Acronyms**

| | |
|---|---|
| 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 |

# 15. 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, Date: 06-December-2023
6. *Functional Package for Secure Shell (SSH),* Version: 1.0, Date: 13-May-2021
7. *CAE MPIC v3.5 Security Target,* Version 1.11, May 2025
8. *CAE MPIC v3.5 Common Criteria Guide,* Version 1.2, May 2025
9. *Getting Started with MPIC Developer's Guide*, TPD 20365 Rev9, 07 October 2024
10. *CAE MPIC v3.5 Assurance Activity Report*, Version 1.6, May 2025
11. *CAE MPIC v3.5 NDcPPv3.0e Vulnerability Assessment*, Version 1.6, May 2025
12. *CAE MPIC v3.5 Evaluation Technical Report*, Version 1.5, May 2025
13. *CAE MPIC v3.5 NDcPPv3.0e Detailed Test Report*, Version 1.5, May 2025
14. *CAE MPIC v3.5 NDcPPv3.0e Test Evidence*, Version 1.3, May 2025