National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0

Report Number: CCEVS-VR-VID11469-2025
Dated: February 10, 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

Farid Ahmed

Anne Gugel

Robert Wojcik

Johns Hopkins Applied Physics Lab

Jerome Myers

Aerospace Corporation

Common Criteria Testing Laboratory

Nathan Bennett

Kevin Steiner

Lightship Security, USA

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 solution provided by UD info. 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 February 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 Full Drive Encryption - Encryption Engine Version 2.0 + Errata 20190201.

The TOE is the UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0. 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 *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 Security Target*, Version 1.2 January 2025 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 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.

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	UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0
Sponsor and Developer	UD info Corporation 3F-4, No. 8, Ln. 609, Sec. 5, Chongxin Rd., Sanchong Dist., New Taipei City 241, Taiwan
CCTL	Lightship Security USA 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.

Item	Identifier
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.
Protection Profile	collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019
ST	UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 Security Target, Version 1.2 January 2025
Evaluation Technical Report	UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 Evaluation Technical Report, Version 1.2 January 2025
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Lightship USA: Nathan Bennett, Kevin Steiner
CCEVS Validators	Johns Hopkins Applied Physics Lab: Farid Ahmed, Anne Gugel, Robert Wojcik Aerospace Corporation: Jerome Myers

3. Architectural Information

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

The TOE is a solid state self-encrypting drive that provides encryption and decryption of stored user data.

3.1. TOE Evaluated Configuration

The TOE evaluated configuration includes the UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0.

Drive	Hardware (HW) P/N	Controller	FW Version
2.5-inch SATA NAND Flash SSD	HF3-25DA128GB-A8P	PS3112-S12	SCPU13.0
	HF3-25DA256GB-A8P		
	HF3-25DA512GB-A8P		
	HF3-25DA001TB-A8P		
	HF3-25DA002TB-A8P		
	HF3-25DA256GB-B8P	PS3112-S12	SCQU15.0
	HF3-25DA512GB-B8P		
	HF3-25DA001TB-B8P		
	HF3-25DA002TB-B8P		
	HF3-25DA004TB-B8P		
M.2 2280 SATA NAND Flash SSD	M2S-80DA128GB-A8P	PS3112-S12	SCPU13.0
	M2S-80DA256GB-A8P		
	M2S-80DA512GB-A8P		
	M2S-80DA001TB-A8P		

Drive	Hardware (HW) P/N	Controller	FW Version
	M2S-80DA002TB-A8P		
	M2S-80DA256GB-B8P	PS3112-S12	SCQU15.0
	M2S-80DA512GB-B8P		
	M2S-80DA001TB-B8P		
	M2S-80DA002TB-B8P		
M.2 2280 NVMe NAND Flash SSD	M2P-80DA256GB-A8P	PS5012-E12	ECPU13.0
	M2P-80DA512GB-A8P		
	M2P-80DA001TB-A8P		
	M2P-80DA002TB-A8P		
	M2P-80DA256GB-BEP	PS5012-E12	ECQU15.0
	M2P-80DA512GB-BEP		
	M2P-80DA001TB-BEP		
	M2P-80DA002TB-BEP		

3.2. Physical Boundary

The physical boundary of the TOE encompasses the UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 firmware running on the SEDs. The TOE hardware is delivered to customers via trusted courier with the firmware preinstalled.

The TOE models support either Non-Volatile Memory Express Peripheral Component Interconnect Express (NVMe PCIe) or Serial Advanced Technology Attachment (SATA) III interfaces. All TOE models incorporate an ARM Cortex-R5 processor (ARMv7-R microarchitecture).

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

The TOE operates with the following components in the environment:

- Authorization Acquisition. Trusted Computing Group Opal (TCG OPAL) v2.0 compliant PBA software installed on a 128 MB read-only Shadow Master Boot Record (MBR) partition on the SED. This is the AA component that supplies the Border Encryption Value (BEV) for locking and unlocking the drives. The AA software provides the Graphical User Interface (GUI) used for performing the security management functions described within the ST.
    - Testing performed using KLC CipherDriveOne v2.0.1
- Protected OS. The TOE supports protection of commonly used operating systems, such as Linux Operating Systems/Linux based Hypervisors and Windows Operating Systems.
- Computer Hardware. Intel based UEFI booted systems that supports Intel Secure Key Technology. CC Testing performed using CPUs:
    - Intel Core i5-13500 (Raptor Lake)
    - Intel® Core™ i5-8400

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Data Protection

The TOE enables encryption and decryption of user data on a SED to protect it from unauthorized disclosure.

4.2. Secure Key Material

The TOE ensures key material used for storage encryption is properly generated and protected from disclosure. It also implements cryptographic key and key material

destruction during transitioning to a Compliant power saving state, or when all keys and key material are no longer needed.

4.3. Secure Management

The TOE enables management of its security functions, including:

i) Changing and erasing the Data Encryption Key (DEK)

ii) Updating the TOE firmware

4.4. Trusted Update

The TOE ensures the authenticity and integrity of firmware updates through digital signatures using Rivest Shamir Adleman Algorithm (RSA) 2048 with Secure Hash Algorithm (SHA)-256.

4.5. Self-Testing

The TOE ensures its integrity and operation by performing self-tests.

4.6. Cryptographic Operations

The TOE performs cryptographic operations as shown in relevant Cryptographic Algorithm Validation Program (CAVP) certificates.

5. Assumptions

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

- *collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata 20190201, February 1, 2019

That information has not been reproduced here and CPP_FDE_EE_V2.0E should be consulted if there is interest in that material.

6. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_FDE_EE_V2.0E as described for this TOE in the Security Target. 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 assurance

activities specified in the CPP_FDE_EE_V2.0E 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.
- 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_FDE_EE_V2.0E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. In particular, as prescribed in sections 2.4.2 and 2.4.3 of the Security Target, the evaluation of the TOE does not include the Authorization Acquisition component which is restricted to the environment nor does it include configurations with multiple disks.

7. Documentation

The following guidance document is provided with the TOE:

- *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 Common Criteria Guide,* Version 1.1, January 2025

This is the only document that should be trusted for the configuration, administration, and use of the product in its evaluated configuration.

IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 FDE Encryption Engine Test Plan*, which is not publicly available. The *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 Assurance Activity Report*, Version 1.2 January 2025 provides an overview of testing and the prescribed assurance activities.

7.1. Developer Testing

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

7.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA lab in Baltimore, MD during April 2024 and August 2024. Remote observation testing was performed and attended by the vendor, evaluation team, validation team and NIAP CCEVS in September 2024. 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 Assurance Activities.

Each Assurance 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 the tables.

Table 2: Devices in the Testing Environment

TOE model	Platform	Controller	Firmware	SFRs
HF3-25DA128GB-A8P	Windows 11, Intel i5-13500	PS3112-S12	SCPU13.0	FCS_VAL_EXT.1 FMT_SMF.1 FPT_TUD_EXT.1
M2P-80DA256GB-A8P	Windows 11, Intel i5-13500	PS5012-E12	ECPU13.0	FCS_VAL_EXT.1 FMT_SMF.1 FPT_TUD_EXT.1

TOE model	Platform	Controller	Firmware	SFRs
M2S-80DA256GB-B8P	Windows 11, Intel i5-13500	PS3112-S12	SCQU15.0	FCS_VAL_EXT.1 FMT_SMF.1 FPT_TUD_EXT.1
M2P-80DA256GB-BEP	Windows 11, Intel i5-13500	PS5012-E12	ECQU15.0	FCS_VAL_EXT.1 FMT_SMF.1 FPT_TUD_EXT.1
HF3-25DA128GB-A8P	Ubuntu 16.04 LTS, Intel® Core™ i5-8400	PS3112-S12	SCPU13.0	FCS_CKM.4(b) FCS_CKM.1(c) FDP_DSK_EXT.1
M2S-80DA256GB-B8P	Ubuntu 16.04 LTS, Intel® Core™ i5-8400	PS3112-S12	SCQU15.0	FCS_CKM.4(b) FCS_CKM.1(c) FDP_DSK_EXT.1
M2P-80DA256GB-A8P	Ubuntu 20.04.2 LTS, Intel® Core™ i5-8400	PS5012-E12	ECPU13.0	FCS_CKM.4(b) FCS_CKM.1(c) FDP_DSK_EXT.1
M2P-80DA256GB-BEP	Ubuntu 20.04.2 LTS, Intel® Core™ i5-8400	PS5012-E12	ECQU15.0	FCS_CKM.4(b) FCS_CKM.1(c) FDP_DSK_EXT.1

Table 3: Tools Used for Testing

Tool name	Version	Description
KLC CipherDriveOne	V2.0.1	This tool provides GUI access to the TOE to be able to perform management functions
Phison Pattern System (for HF3-25DA128GB-A8P and M2S-80DA256GB-B8P)	0.9.01.33	This tool was used to test the deletion and generation of key as well as provide

Tool name	Version	Description
		dumps of the entire drive to verify evidence
Phison Pattern System (for M2P-80DA256GB-A8P and M2P-80DA256GB-BEP)	1.10.01.01	This tool was used to test the deletion and generation of key as well as provide dumps of the entire drive to verify evidence
DLMC Tool for Trusted Update	V1.00	This tool was used for updating the firmware on the TOE for trusted update tests.
HxD	2.5.0.0	This tool was used to verify binary file dumps with key contents

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 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 the UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in CPP_FDE_EE_V2.0E.

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 UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 products 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 documents. Additionally, the evaluator performed the assurance activities specified in the CPP_FDE_EE_V2.0E 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. 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.

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 CPP_FDE_EE_V2.0E 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.

8.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 CPP_FDE_EE_v2.0E Vulnerability Assessment*, Version 1.1, January 2025, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on January 10, 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

The Evaluation team performed a search using the following keywords:

- HF3-25DA128GB-A8P
- HF3-25DA256GB-A8P
- HF3-25DA512GB-A8P

- HF3-25DA001TB-A8P
- HF3-25DA002TB-A8P
- HF3-25DA256GB-B8P
- HF3-25DA512GB-B8P
- HF3-25DA001TB-B8P
- HF3-25DA002TB-B8P
- HF3-25DA004TB-B8P
- M2S-80DA128GB-A8P
- M2S-80DA256GB-A8P
- M2S-80DA512GB-A8P
- M2S-80DA001TB-A8P
- M2S-80DA002TB-A8P
- M2S-80DA256GB-B8P
- M2S-80DA512GB-B8P
- M2S-80DA001TB-B8P
- M2S-80DA002TB-B8P
- M2P-80DA256GB-A8P
- M2P-80DA512GB-A8P
- M2P-80DA001TB-A8P
- M2P-80DA002TB-A8P
- M2P-80DA256GB-BEP
- M2P-80DA512GB-BEP
- M2P-80DA001TB-BEP
- M2P-80DA002TB-BEP
- UDinfo SSD
- SCPU13.0
- SCQU15.0
- ECPU13.0
- ECQU15.0
- cpe:2.3:h:arm:arm7:-:*:*:*:*:*:*:*:*
- cpe:2.3:h:arm:cortex-r:-:*:*:*:*:*:*:*:*
- PS5012-E12
- PS3112-S12
- drive encryption
- disk encryption
- key destruction
- key sanitization
- Self Encrypting Drive
- SED
- OPAL
- ARM Cortex-R5

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 and performed the Assurance Activities in the CPP_FDE_EE_V2.0E 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 7 of this Validation Report. 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. 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.

10. Annexes

Not applicable.

11. Security Target

UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 Security Target, Version 1.2 January 2025.

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
ETR	Evaluation Technical Report
IT	Information Technology
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 Full Drive Encryption – Encryption Engine*, Version 2.0e + Errata 20190201, February 1, 2019
6. *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 Security Target*, Version 1.2 January 2025
7. *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 Common Criteria Guide*, Version 1.1, January 2025
8. *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 Assurance Activity Report*, Version 1.2 January 2025
9. *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 CPP_FDE_EE_v2.0E Vulnerability Assessment*, Version 1.1, January 2025
10. *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 Evaluation Technical Report*, Version 1.2, January 2025
11. *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 FDE Encryption Engine Test Plan*, Version 1.2 January 2025
12. *UD info SSD Drives, Firmware Versions: SCPU13.0/ECPU13.0/SCQU15.0/ECQU15.0 FDE Encryption Engine Test Plan Evidence*, Version 1.0, November 2024