ASSURANCE CONTINUITY MAINTENANCE REPORT FOR KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 and SCPB15.0/ECPB15.0

KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 and SCPB15.0/ECPB15.0

Maintenance Report Number: CCEVS-VR-VID11453-2026

Date of Activity: 03 June 2026

References:

- *Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation*, version 3.0, 12 September 2016
- *KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 and SCPB15.0/ECPB15.0 Impact Analysis Report #2*, Version 1.2, June 2026
- *Collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0, February 1, 2019

10 March 2025 Assurance Maintenance Documentation:

- *KLC Advantech Drives Firmware Version: SCPB15.0/ECPB15.0 Security Target*, Version 2.0, January 2025
- *KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 Common Criteria Guide*, Version 2.0, January 2025
- *Assurance Continuity Maintenance Report for KLC Advantech Drives Firmware Version: SCPB15.0/ECPB15.0*, CCEVS-VR-VID11453-2025, 10 March 2025

Maintained Documentation:

- *KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 and SCPB15.0/ECPB15.0 Security Target*, Version 3.1, May 2026
- *KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 and SCPB15.0/ECPB15.0 Common Criteria Guide, Version 3.0*, May 2026

Assurance Continuity Maintenance Report:

Lightship Security USA, Inc. submitted an Impact Analysis Report (IAR) for the KLC Advantech Drives, Firmware Version: SCPB13.0/ECPB13.0 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 22 May 2026. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those

requirements, the IAR describes the changes made to the certified Target of Evaluation (TOE), the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consists of the original evaluation Security Target (ST) and Administrator's Guide (AGD) and the IAR. In addition, previous assurance maintenance documentation was reviewed (see above for a full list of documentation). The ST and AGD were updated to the new version of the TOE.

The information below has all been compiled based on the IAR, updated ST and updated AGD provided for this assurance maintenance.

Documentation updated:

Original CC Evaluation Evidence	Evidence Change Summary

Security Target:
KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 Security Target, Version 1.4, June 2024
	Maintained Security Target:
	See references above.
	The ST has been revised to update the following:
	• Title Page
	• ST Reference
	• TOE Reference
	• Terminology table (to include BiCS (Bit Cost Scalable))
	• Guidance document version
	• 'TOE Hardware / Firmware' table to:
	  o categorize by BiCS Type;
	  o include 2 TB capacity models;
	  o update the nomenclature to associate models with the re-introduced Firmware 13.0 versions;
	  o align BiCS5 models with the 15.0 Firmware versions; and
	  o remove obsolete capacity models.

Design Documentation: See ST and Guidance Documentation.	See ST and Guidance changes in this table. No changes to the Key Management Description (KMD) were required and, therefore, are not included.
Guidance Documentation: *KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 Common Criteria Guide*, Version 1.1, June 2024	**Maintained Guidance Documentation:** See references above. The AGD has been revised to update the following: • Title Page • Terminology table (to include BiCS) • 'TOE Hardware / Firmware' table to: o categorize by BiCS Type;

	○ include 2 TB capacity models; ○ update the nomenclature to associate models with the re-introduced Firmware 13.0 versions; ○ align BiCS5 models with the 15.0 Firmware versions; and ○ remove obsolete capacity models.
Lifecycle: None	No changes required.
Testing: None	No additional testing required. As provided in more detail below, Firmware versions SCPB13.0/ECPB13.0 were tested as part of the original evaluation. Versions SCPB15.0/ECPB15.0 were tested as part of the March 2025 Assurance Maintenance activities.
Vulnerability Assessment: None	Lightship Security performed an updated search of public information for potential vulnerabilities on May 20, 2026. No public vulnerabilities exist in the product. See analysis below.

Changes to the TOE:
The TOE Firmware has been updated to include the originally evaluated Firmware SCPB13.0 / ECPB13.0 versions, in addition to the maintained Firmware SCPB15.0 / ECPB15.0 versions. As part of that change, the TOE configuration has been updated to differentiate between BiCS4 and BiCS5 technologies. In addition to the Firmware, variants with additional storage capacity have been added while models that are no longer supported have been removed.

Major Changes
None.

Minor Changes
As summarized above, the following were the changes to the TOE:

TOE configuration/nomenclature - updated to include and distinguish between BiCS4 and BiCS5 memory technologies. (A "-1" suffix has been added to specific hardware part numbers (e.g., SQF-2040-256ECM-1) to identify re-released BiCS4 models.) The TOE identification now reflects two parallel firmware branches based on the underlying hardware generation:

- *BiCS4 Branch* - These models use Firmware Version SCPB13.0 / ECPB13.0, which is part of the initial evaluation baseline.

- *BiCS5 Branch* - These models use the Firmware Version SCPB15.0 / ECPB15.0 branch established in the previous assurance continuity maintenance release.

Capacity Variants - includes expanded storage capacities (2 Terabyte). Legacy 128 and certain 256 Gigabyte models have been removed to reflect current product availability.

There are no changes to hardware controllers. The same controller modules used in the Validated and 10 March 2025 Maintained TOEs for the SCPB13.0/SCPB15.0 firmware (Controller PS3112-S12) and ECPB13.0/ECPB15.0 firmware (Controller PS5012-E12) are maintained in the Changed TOE.

All changes to the TOE are assessed as Minor for the following reasons:

- The distinction between BiCS4 and BiCS5 provides additional clarity but has no impact on security functionality. Both versions were part of either the Validated or 10 March 2025 Maintained TOE. As noted in the 10 March 2025 ACMR, BiCS4 versus BiCS5 is a performance enhancement and has no impact on the cryptographic functionality.
- Expanded storage capacity and removal of legacy models do not impact the security functionality of the TOE.

None of the changes resulted in the introduction of new TOE capabilities, modification to security functions as defined in the ST, or changes to the TOE boundary.

Regression Testing

The developer did not perform new testing activities as part of this maintenance activity as the TOE remains identical to previously validated and maintained versions.
The TOE continues to use the two firmware branches:

- Firmware Version SCPB13.0 and ECPB13.0, which was fully tested in the initial evaluation baseline.
- Firmware Version SCPB15.0 and ECPB15.0, which was fully regression tested and accepted in the previous maintenance release

There have been no changes to the hardware controllers. The updates to storage capacity have no impact on the behavior of the TOE. The security logic, cryptographic boundaries, and external interfaces remain identical. As such, test evidence and results from the initial evaluation and the subsequent maintenance release remain valid and applicable to the Changed TOE.

Equivalency

As noted previously, all Firmware versions were included in the original Validation or previous Maintenance release. There are no new Firmware versions included in this maintenance. In addition, there have been no changes to the underlying hardware controllers. The only change was to add to the model storage capacities, which has no impact on security functionality.

NIST CAVP Certificates:

The CAVP certificate numbers referenced during the original evaluation have not changed and remain applicable to the maintained TOE.

Vulnerability Analysis:
A public search for potential vulnerabilities was performed on May 20, 2026, using the following sources:

- NIST National Vulnerability Database (https://nvd.nist.gov)
- MITRE CVE Search (https://cve.mitre.org/cve/search_cve_list.html)
- CISA - Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

The following search terms were used, which included all models, firmware, controllers, and key terms:

- Drive encryption
- Disk encryption
- Key destruction
- Key sanitization
- Self Encrypting Drive
- SED
- OPAL
- KLC Advantech
- SQF-2020-2TSCB-1
- SQFFS25V8-2TSC-1
- SQF-2020-1TSCB-1
- SQFFS25V8-1TSC-1
- SQF-2020-512SCB-1
- SQFFS25V8-512GSC-1
- SQF-2020-256SCB-1
- SQFFS25V4-256GSC-1
- SQF-2040-2TECM-1
- SQFFCM8V4-2TEC-1
- SQF-2040-1TECM-1
- SQFFCM8V4-1TEC-1
- SQF-2040-512ECM-1
- SQFFCM8V4-512GEC-1
- SQF-2040-256ECM-1
- SQFFCM8V4-256GEC-1
- SQF-2020-2TSCB
- SQFFS25V8-2TSC
- SQF-2020-1TSCB
- SQFFS25V8-1TSC
- SQF-2020-512SCB
- SQFFS25V8-512GSC
- SQF-2020-256SCB
- SQFFS25V4-256GSC
- SQF-2020-1TSCM
- SQFFSM8V4-1TSC
- SQF-2020-512SCM
- SQFFSM8V4-512GSC
- SQF-2040-2TECM
- SQFFCM8V4-2TEC
- SQF-2040-1TECM
- SQFFCM8V4-1TEC
- SQF-2040-512ECM
- SQFFCM8V4-512GEC
- SQF-2040-256ECM
- SQFFCM8V4-256GEC
- PS3112-S12
- PS5012-E12
- ARM Cortex-R5
- cpe:2.3:h:arm:cortex-r:-:*:*:*:*:*:*:*
- cpe:2.3:h:arm:arm7:-:*:*:*:*:*:*:*
- SCPB15.0
- ECPB15.0
- SCPB13.0
- ECPB13.0

No open vulnerabilities applicable to the TOE were identified. All known public security vulnerabilities are mitigated in the TOE version.

Conclusion:
The overall impact of the changes presented for this Assurance Maintenance is minor. This is based on the rationale that updates do not change any security policies of the TOE and are unrelated to SFR claims. The updates described above were made to support both the originally validated and previously maintained versions of the TOE firmware in addition to providing support for additional capacity.

There are no changes to TSF Interfaces, no SFR changes, and no NIST cryptographic certificate changes. Regression testing was not required because the updated TOE being presented for maintenance contained unmodified versions that were tested during the initial evaluation and during the previous maintenance activity. The reasoning is considered adequate based on the types of changes made. The vulnerability search also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. Therefore, CCEVS agrees that the original assurance is maintained for the product.