National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

L3Harris Common Data Loader Version 02.01

Report Number:	**CCEVS-VR-VID11503-2024**
Dated:	**December 23, 2024**
Version:	**1.0**

ACKNOWLEDGEMENTS

Table of Contents

1   Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of L3Harris Common Data Loader solution provided by L3Harris Technologies. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in December 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. 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, February 1, 2019 and collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019.

The Target of Evaluation (TOE) is the L3Harris Common Data Loader Version 02.01.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the L3Harris Common Data Loader Version 02.01 Security Target, version 0.4, December 12, 2024 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 Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.

- The Security Target (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
TOE	L3Harris Common Data Loader Version 02.01 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 and collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019
ST	L3Harris Common Data Loader Version 02.01 Security Target, version 0.4, December 12, 2024
Evaluation Technical Report	Evaluation Technical Report for L3Harris Common Data Loader Version 02.01, version 0.2, December 12, 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	L3Harris Technologies
Developer	L3Harris Technologies
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jerome Myers, Ph.D. Swapna Katikaneni Mike Quintos

3   Architectural Information

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

The Target of Evaluation (TOE) is Common Data Loader Version 02.01.

The TOE provides software Full Drive Encryption of removable memory modules (RMM).

3.1   TOE Description

The L3Harris Common Data Loader Version 02.01 (CDL) is a full-disk encryption solution composed of the Common Data Loader Operational Flight Platform (CDL OFP) software and the Ground Stations Software (CDL GSS).

The CDL Operational Flight Platform is an embedded avionics module for onboard non-volatile, network-attached storage. The TOE provides a layer of software encryption on top of embedded removable memory modules (RMM) inserted into the CDL OFP, which themselves are intended to be external self-encrypting drives (separately evaluated by another vendor). The CDL OFP software is designed to operate on a physical hardware device featuring up to three RMMs, two independent ethernet ports, two RS-232 serial interfaces (one for maintenance and one for debugging), and six discrete inputs including one for zeroization.

The TOE also includes the CDL Ground Station Software, a full, stand-alone software suite capable of provisioning and managing the RMMs used with the CDL OFP. The CDL Ground Station Software includes both the Provisioning Tool used to initialize the Data at Rest solution and the Mission Planning Software used to load encrypted data for a given deployment of the RMMs for use in the CDL OFP. The CDL GSS Provisioning Tool and the CDL GSS Mission Planning Software are designed to run on separate machines as they require different OS support.

The TOE in total consists of three distinct software parts. The three parts in aggregate provide the security functionality laid forth in this document and are evaluated as one solution as the combined TOE solution covers all of the required functionality. The CDL GSS is used to initially provision the FDE solution, configuring any necessary keys and authentication factors, while the CDL OFP and CDL GSS Mission Planning Software are both used to load and retrieve encrypted data on to the protected drives, either from the ground or vehicle deployment respectfully.

The TOE is distributed as a software package designed to work on a specific set of hardware. The TOE has the following hardware/software requirements:

- The Operational Flight Platform requires a computer with a Human Computer Interface (HCI) and a NXP P3041 processor. The tested configuration included a L3Harris-bespoke OFP computer running Buildroot 2012.05 on Linux Kernel 3.5.3 on NxP QorlQ P3041 (e500mc).

- The CDL GSS Provisioning Tool requires a native Ubuntu 20.04 LTS computer with eSATA port (or equivalent USB adapter). The tested configuration ran the CDL GSS

Provisioning Tool software on a laptop running native Ubuntu 20.04 and Linux Kernel 5.4.0-1091-fips with an Intel Haswell i7-4810MQ.

- The CDL GSS Mission Planning Software requires an Ubuntu 22.04 LTS computer with eSATA port (or equivalent USB adapter). The tested configuration ran the CDL GSS Mission Planning Software on a laptop running Ubuntu 22.04.2 LTS with Linux Kernel 5.15.90.1 through Windows Subsystem for Linux (WSL) 2 on an Intel Haswell i7-4810MQ.

Because the CDL GSS software (both the Provisioning Tool Mission Planning Software) do not rely on any hardware acceleration and the OS provides a hardware abstraction layer, the CDL GSS software executes identically irrespective of the underlying CPU. Additionally, the tested configuration utilized the separately evaluated Novachips Co., Ltd. Scalar and Express P-series SSD, version NV.R1900 RMM units to provide the second layer of hardware full-disk encryption.

The TOE features several network protocols such as Network File System (NFS), Real Time Protocol (RTP) and Real time Streaming Protocol (RTSP) which are not tested as a part of this evaluation. The FDEEEcPP20E and FDEAAcPP20E Protection Profiles did not consider nor include networking protocols as part of the security functional requirements, and thus did not include any such protocol requirements. Therefore, these protocols have not been examined as part of the required assurance activities and consequently the evaluation can make no claims about the TOE's networking protocols.

3.2 TOE Architecture

The TOE provides a software Full Drive Encryption solution that can accept up to three Removable Memory Module (RMM), each containing their own data drive.

3.3 Physical Boundaries

The Ground Station Software's physical boundary is the boundary of the software package distributed by the vendor. Similarly, the CDL OFP physical boundary is the software package distributed by the vendor, however the CDL OFP also utilizes a kernel cryptography library on the Operational Flight Platform that utilizes P3041-based hardware acceleration. Because of this, the TOE also includes the compatible NXP CPU hardware within its physical boundary. In total, the TOE's physical boundary is the boundary of the software packages for both the CDL OFP and GSS with the addition of the NXP processor hardware on the CDL OFP. Together, the components of the TOE provide a full solution to secure Data at Rest (DAR).

4 Security Policy

This section summaries the security functionality of the TOE:
1. Cryptographic support
2. User data protection

3. Security management
4. Protection of the TSF

4.1 Cryptographic support

The TOE includes cryptographic functionality for key management, user authentication, and block-based encryption including: symmetric key generation, encryption/decryption, cryptographic hashing, keyed-hash message authentication, and password-based key derivation.   These functions are supported with suitable random bit generation, key derivation, salt generation, initialization vector generation, secure key storage, and key destruction.   These primitive cryptographic functions are used to encrypt Data at Rest (including the generation and protection of keys and key encryption keys) used by the TOE.

4.2 User data protection

The TOE performs Full Drive Encryption on all partitions on the drive (so that no plaintext exists) and does so without user intervention.

4.3 Security management

The TOE provides each of the required management services necessary to manage the full drive encryption using a command line interface.

4.4 Protection of the TSF

The TOE implements a number of features to protect itself to ensure the reliability and integrity of its security features. It protects key and key material, and includes functions to perform self-tests and software/firmware integrity checking so that it might detect when it is failing or may be corrupt. If any of the self-tests fail, the TOE will not go into an operational mode.

5 Assumptions & Clarification of Scope

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

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

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

That information has not been reproduced here and the FDEAAcPP20E/FDEEEcPP20E should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the FDEAAcPP20E/FDEEEcPP20E 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.

Clarification of scope

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 Full Drive Encryption Protection Profiles 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, additional customer documentation for the specific Full Drive Encryption models was not included in the scope of the evaluation and therefore should not to 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 FDEAAcPP20E/FDEEEcPP20E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Administrative Guide: Common Data Loader (CDL) Data-At-Rest (DAR) Operational Flight Platform (OFP) and Ground Support Software (GSS), Version 1.0, October 7, 2024

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 to 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 Detailed Test Report for L3Harris Common Data Loader, Version 0.2, December 12, 2024 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

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 verified the product according to a Common Criteria Certification document and ran the tests specified in the FDEAAcPP20E/FDEEEcPP20E including the tests associated with optional requirements. Section 1 of the AAR identifies the tested device, and a diagram of the test environment with a list of test tools is provided in Section 3.3.

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 ETR. 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 Common Data Loader TOE to be Part 2 extended, and to meet the SARs contained in the FDEAAcPP20E/FDEEEcPP20E.

8.1   Evaluation of the 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 L3Harris Common Data Loader Version 02.01 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

8.2   Evaluation of the Development (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 Security Target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the FDEAAcPP20E/FDEEEcPP20E related to the examination of the information contained in the TSS.

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

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

8.4   Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

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

8.5   Evaluation of the 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 FDEAAcPP20E/FDEEEcPP20E and recorded the results in a Test Report, summarized in the AAR.

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

8.6   Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes

a public search for vulnerabilities. The search was performed on December 12, 2024, and a summary is included in Section 3.4 of the AAR. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: "L3Harris", "Common Data Loader", "Operational Flight Platform", "Ground Station Software", "Drive encryption", "Disk encryption", "Key destruction", "Key santization", "Opal managment software", "SED management software", "Key caching", "LUKS", "kernel cryptography", "Linux 5.4.0", "Linux 5.15.9", "Windows 10", "Windows Subsystem for Linux", "Ubuntu 22.04", "Debian", "L3Harris Common Data Loader OFP 02.01.00 ", "L3Harris Mission Planning Software 02.01.00 ", and "L3Harris Provisioning Tool 02.01.00.

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

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 testing 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 correctly verified that the product meets the claims in the ST.

9   Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the guidance document listed in Section 6. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Remote management of the TOE is outside the scope of this evaluation. Administration of the TOE must be performed locally over a simple connection in the evaluated configuration.

Other functionality included in the product, including network protocols such as Network File System (NFS), Real Time Protocol (RTP), and Real Time Streaming Protocol (RTSP), were not assessed as part of this evaluation. No other versions of the TOE, either earlier or later, were evaluated.

Additional functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other items and scope issues have been sufficiently addressed in other sections of this document.

10 **Annexes**

Not applicable

11 **Security Target**

The Security Target is identified as: *L3Harris Common Data Loader Version 02.01 Security Target, Version 0.4, December 12, 2024*.

12 **Glossary**

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.

- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

- **Feature.** Part of a product that is either included with the product or can be ordered separately.

- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 **Bibliography**

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

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019.

[5] collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019.

[6] L3Harris Common Data Loader Version 02.01 Security Target, Version 0.4, December 12, 2024 (ST).

[7] Assurance Activity Report for L3Harris Common Data Loader Version 02.01, Version 0.2, December 12, 2024 (AAR).

[8] Detailed Test Report for L3Harris Common Data Loader Version 02.01, Version 0.2, December 12, 2024 (DTR).

[9] Evaluation Technical Report for L3Harris Common Data Loader Version 02.01, Version 0.2, December 12, 2024 (ETR).