



CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT
ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer version 5.5

Maintenance Report Number: CCEVS-VR-VID11354-2025

Date of Activity: March 20, 2025

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." 29 August 2014.

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer version 5.5 Security Target, Version 1.8, February 25, 2025

Impact Analysis Report for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer version 5.5, Version 1.1, March 18, 2025

collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201 (CPP_FDE_AA_V2.0E)

collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201 (CPP_FDE_EE_V2.0E)

Affected Evidence:

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer version 5.4 Security Target, version 1.7, 03/21/2023

Updated Developer Evidence:

This assurance maintenance request is to update the TOE to incorporate one bug fix. The developer has provided sufficient supporting rationale describing the impact of this change. The Security Target was updated to identify the new TOE version.

Description of ASE Changes:

Gossamer Security Solutions (GSS) submitted an Impact Analysis Report (IAR #1) to CCEVS, on behalf of Curtiss-Wright Defense Solutions for approval update the TOE to incorporate one bug fix.

Changes to TOE:

The only change to the TOE was an update from version 5.4 to version 5.5 to incorporate one bug fix. This update was implemented to fix the functionality of a Command Line Interface (CLI) command option to behave as expected. This change does not affect the security functionality of the TOE.

Description of ALC Changes:

1. Security Target – The Security Target has been updated to identify the new TOE version. No other changes were necessary to the Security Target as this change was minor and did not impact the ST.

Assurance Continuity Maintenance Report:

- GSS submitted an Impact Analysis Report (V1.1), on behalf of Curtiss-Wright Defense Solutions to update the TOE from version 5.4 to 5.5.
- Updates consist of one bug fix.
- There are no security relevant fixes, so no new certification is required.
- No development environment changes occurred that impacted the product.
- There were no changes that required the evaluators to do any additional testing.

Description of Regression Testing:

Curtiss Wright performs regression testing on each product version. This includes low level testing designed to address any CC related issues.

Each release must go through a series of tests which Curtiss Wright terms ATP or Acceptance Test Procedure which tests all supported capability/features (NAS, PXE, iSCSI, PCAP, etc.) and operations, utilizing both encryption layers: HWFDE and SWFDE, to ensure that they maintain the integrity of the product. In other words, Curtiss Wright wants to ensure that any given release complies with customer expectation and does not break the existing functionality. It is also tested to ensure that developers are not introducing new bugs with each release.

CAVP Analysis:

The CAVP analysis performed in the original evaluation remains valid as no crypto libraries have changed and the hardware remains unchanged. The only change was unrelated to any algorithm certificates.

Vulnerability Assessment:

The public vulnerability search was updated from 3/13/2023. The evaluator searched the following public vulnerability databases:

- National Vulnerability Database (<https://web.nvd.nist.gov/vuln/search>)
- Vulnerability Notes Database (<http://www.kb.cert.org/vuls/>)

with the following search terms:

- "Disk encryption"
- "Drive encryption"
- "Key destruction"
- "Key sanitization"
- "Opal management software"
- "SED management software"
- "Password caching"
- "Key caching"
- "Curtiss Wright"
- "Defense Solutions Data Transport System"
- "Curtiss Wright Crypto Firmware"
- "NXP (Phillips) ARM7 Processor P/N LPC2368FBD100"
- "Maxim Integrated DS3645"
- "Microchip ATECC508A"
- "Enova X-Wall MX-256C",

The IAR contains the output from the vulnerability searches and the rationale why the search results are not applicable to the TOE. This search was performed on February 24, 2025. No vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

There has been a minor product change to update a command to reflect the documented behavior. The ST has been updated to reflect the new version. The Guidance document has not been updated as it was not needed.

Note that Curtiss Wright continually tracks bugs, vulnerabilities, and other defects reported in the public domain and at the time of this report there are no known outstanding security-related vulnerabilities in the TOE.

Validation Team Conclusion:

The validation team reviewed the changes and concurred the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The updated Security Target changed to update the TOE version.

Based on this and other information from within this IAR document, the Validation Team agrees that the assurance impact of these changes is minor.