National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition

Version 2.0 + Errata 20190201

26 April 2019

Report Number: CCEVS-VR-PP-0049
Dated: 26 April 2019
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base and Additional Requirements
Gossamer Security Solutions Common Criteria Testing Laboratory
Catonsville, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 (FDEAAcPP). It presents a summary of the FDEAAcPP and the evaluation results.

The evaluation of the FDEAAcPP was performed concurrent with the first product evaluation against the cPP's requirements. In this case the Target of Evaluation (TOE) was the:

1. Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer, performed by Gossamer Security Solutions in Catonsville, Maryland, United States of America.

This evaluation addressed the base requirements of the FDEAAcPP, as well as most of the additional requirements contained in Appendices A and B.

An additional review of the cPP was performed independently by the Validation Report (VR) author as part of the completion of this VR, to confirm that it meets the claimed APE assurance requirements.

The evaluation determined that the FDEAAcPP is both Common Criteria Part 2 Extended and Part 3 Conformant. The cPP identified in this VR has been evaluated at NIAP approved CCTLs 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). Because the ST contains only material drawn directly from the FDEAAcPP, the majority of the ASE work units served to satisfy the APE work units as well.

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 evaluation technical report are consistent with the evidence provided.

The initial results by the validation team found that the evaluation showed that the FDEAAcPP did not meet the requirements of the APE components. These findings were confirmed by the VR author and NIAP. NIAP notified the Full Disk Encryption international Technical Community (FDE iTC) of all noted deficiencies. The FDE iTC determined the impact of the changes were minor. The majority of the changes were typographical errors related to the conventions for indicating assignments and selections and there was one dependency SFR missing. Subsequently, the FDE iTC corrected all deficiencies and published the FDEAAcPP 2.0 + Errata 20190201. NIAP reviewed the Errata and confirmed all changes were made. As a result, the validation team found that the evaluation showed that the FDEAAcPP 2.0 + Errata 20190201 meets the requirements of the APE components.

NIAP also reviewed each previously evaluated product and confirmed the changes had a minor impact on the security functionality of the products. Both evaluations addressed the changes through Assurance Continuity process. Therefore, the evaluated products also comply with the FDEAAcPP 2.0 + Errata 20190201. Note that this is true despite the fact that the FDEAAcPP 2.0 + Errata 20190201 conforms to Common Criteria v3.1, Release 5, while the previous FDEAAcPP 2.0 conformed to Release 4; the changes between releases did not impact the relevant evaluations.

.

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 CCTLs. CCTLs evaluate products against cPPs that contain Assurance Activities, which are interpretations of CEM work units specific to the technology described by the cPP.

In order to promote thoroughness and efficiency, the evaluation of the FDEAAcPP was performed concurrent with the first product evaluation against the cPP's requirements. In this case the Target of Evaluation (TOE) was the:

1. Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer, performed by Gossamer Security Solutions in Catonsville, Maryland, United States of America.

This evaluation addressed the base requirements of the FDEAAcPP, as well as most of the additional requirements contained in Appendices A and B.

The FDEAAcPP contains a set of "base" requirements that all conformant STs must include, and additionally contains "Optional" and "Selection-based" requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in the base requirements and the capabilities of the TOE.

Because these discretionary requirements may not be included in a particular ST, the initial use of the cPP will address (in terms of the cPP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the FDEAAcPP that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made when that occurs.

The following identifies the cPP subject of the evaluation/validation, as well as the supporting information from the evaluation performed against this cPP and any subsequent evaluations that address additional optional and/or selection-based requirements in the FDEAAcPP.

Protection Profiles	Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0, 09 September 2016
	Collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019
ST (Base)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer (FDEEEcPP20/FDEAAcPP20) Security Target, Version 0.6, 18 October 2018

Assurance Activity Report (Base)	Assurance Activity Report (FDEEEcPP20/FDEAAcPP20) for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer, Version 0.3, 18 October 2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTLs	Gossamer Security Solutions, Catonsville, MD, USA

3 FDEAAcPP Description

The FDEAAcPP specifies information security requirements for Full Drive Encryption – Authorization Acquisition, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

A full drive encryption authorization acquisition in the context of the cPP is a device composed of hardware and/or software that may be either a Host software solution that manages a HW Encryption Engine (e.g. a SED) or as part of a combined evaluation of this cPP and the Encryption Engine cPP for a vendor that is providing a solution that includes both components. The FDEAAcPP describes the requirements for the Authorization Acquisition and details the security requirements and assurance activities necessary to interact with a user and result in the availability of sending a Border Encryption Value (BEV) to the Encryption Engine. The FDEAAcPP also includes a set of core requirements for management functions, proper handling of cryptographic keys, updates performed in a trusted manner, audit and self-tests.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
A.INITIAL_DRIVE_STATE	Users enable Full Drive Encryption on a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption. The cPP does not intend to include requirements to find all the areas on storage devices that potentially contain protected data. In some cases, it may not be possible - for example, data contained in "bad" sectors. While inadvertent exposure to data contained in bad sectors or un-partitioned space is unlikely, one may use forensics tools to recover data from such areas of the storage device. Consequently, the cPP assumes bad sectors, un-partitioned space, and areas that must contain unencrypted code (e.g., MBR and AA/EE pre-authentication software) contain no protected data.

A.SECURE_STATE	Upon the completion of proper provisioning, the drive is only assumed secure when in a powered off state up until it is powered on and receives initial authorization.
A.TRUSTED_CHANNEL	Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure. In cases in which a single product fulfils both cPPs, then the communication between the components does not extend beyond the boundary of the TOE (e.g., communication path is within the TOE boundary). In cases in which independent products satisfy the requirements of the AA and EE, the physically close proximity of the two products during their operation means that the threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.
A.TRAINED_USER	Authorized users follow all provided user guidance, including keeping password/passphrases and external tokens securely stored separately from the storage device and/or platform.
A.PLATFORM_STATE	The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.
A.SINGLE_USE_ET	External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.
A.POWER_DOWN	The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off, so memory remnant attacks are infeasible. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen). Users power the platform and/or storage device down or place it into a power managed state, such as a “hibernation mode”.
A.PASSWORD_STRENGTH	Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.
A.PLATFORM_I&A	The product does not interfere with or change the normal platform identification and authentication functionality such as the operating system login. It may provide authorization factors to the operating system's login interface, but it will not change or degrade the functionality of the actual interface.
A.STRONG_CRYPTO	All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG.
A.PHYSICAL	The platform is assumed to be physically protected in its Operational Environment and not subject to physical attacks that compromise the security and/or interfere with the platform’s correct operation.

4.2 Threats

The following table contains applicable threats.

Table 2: Threats

Threat Name	Threat Definition
T.UNAUTHORIZED_DATA _ACCESS	The cPP addresses the primary threat of unauthorized disclosure of protected data stored on a storage device. If an adversary obtains a lost or stolen storage device (e.g., a storage device contained in a laptop or a portable external storage device), they may attempt to connect a targeted storage device to a host of which they have complete control and have raw access to the storage device (e.g., to specified disk sectors, to specified blocks).
T.KEYING_MATERIAL_COMPROMISE	Possession of any of the keys, authorization factors, submasks, and random numbers or any other values that contribute to the creation of keys or authorization factors could allow an unauthorized user to defeat the encryption. The cPP considers possession of key material of equal importance to the data itself. Threat agents may look for key material in unencrypted sectors of the storage device and on other peripherals in the operating environment (OE), e.g. BIOS configuration, SPI flash.
T.AUTHORIZATION_GUESSING	Threat agents may exercise host software to repeatedly guess authorization factors, such as passwords and PINs. Successful guessing of the authorization factors may cause the TOE to release BEV or otherwise put it in a state in which it discloses protected data to unauthorized users.
T.KEYSPACE_EXHAUST	Threat agents may perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms and/or parameters allow attackers to exhaust the key space through brute force and give them unauthorized access to the data.
T.UNAUTHORIZED_UPDATE	Threat agents may attempt to perform an update of the product which compromises the security features of the TOE. Poorly chosen update protocols, signature generation and verification algorithms, and parameters may allow attackers to install software and/or firmware that bypasses the intended security features and provides them unauthorized access to data.

4.3 Organizational Security Policies

The following table contains applicable organizational security policies.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
There are no listed organizational security policies for the TOE.	

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
There are no listed security objectives for the TOE.	

The following table contains security objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Obj.	Environmental Security Objective Definition
OE.TRUSTED_CHANNEL	Communication among and between product components (i.e., AA and EE) is sufficiently protected to prevent information disclosure.
OE.INITIAL_DRIVE_STATE	The OE provides a newly provisioned or initialized storage 15 device free of protected data in areas not targeted for encryption.
OE.PASSPHRASE_STRENGTH	An authorized administrator will be responsible for ensuring that the passphrase authorization factor conforms to guidance from the Enterprise using the TOE.
OE.POWER_DOWN	Volatile memory is cleared after power-off so memory remnant attacks are infeasible.
OE.SINGLE_USE_ET	External tokens that contain authorization factors will be used for no other purpose than to store the external token authorization factor.
OE.STRONG_ENVIRONMENT_CRYPTO	The Operating Environment will provide a cryptographic function capability that is commensurate with the requirements and capabilities of the TOE and Appendix A.
OE.TRAINED_USERS	Authorized users will be properly trained and follow all guidance for securing the TOE and authorization factors.
OE.PLATFORM_STATE	The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.
OE.PLATFORM_I&A	The Operational Environment will provide individual user identification and authentication mechanisms that operate independently of the authorization factors used by the TOE.
OE.PHYSICAL	The Operational Environment will provide a secure physical computing space such than an adversary is not able to make modifications to the environment or to the TOE itself.

5 Requirements

As indicated above, requirements in the FDEAAcPP are comprised of the "base" requirements and additional requirements that are conditionally optional. The following table contains the "base" requirements that were validated as part of the Curtis Wright Defense evaluation activity referenced above.

Table 6: Base Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_AFA_EXT.1: Authorization Factor Acquisition	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer

	FCS_AFA_EXT.2: Timing of Authorization Factor Acquisition	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_CKM.4(a): Cryptographic Key Destruction (Power Management)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_CKM.4(d): Cryptographic Key Destruction (Software TOE, 3rd Party Storage)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_CKM_EXT.4(a): Cryptographic Key and Key Material Destruction (Destruction Timing)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_CKM_EXT.4(b): Cryptographic Key and Key Material Destruction (Power Management)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_KYC_EXT.1: Key Chaining (Initiator)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_SNI_EXT.1: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
FMT: Security Management	FMT_MOF.1: Management of Functions Behavior	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FMT_SMF.1: Specification of Management Functions	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FMT_SMR.1: Security Roles	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
FPT: Protection of the TSF	FPT_KYP_EXT.1: Protection of Key and Key Material	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FPT_PWR_EXT.1: Power Saving States	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FPT_PWR_EXT.2: Timing of Power Saving States	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FPT_TUD_EXT.1: Trusted Update	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if

associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
FPT: Protection of the TSF	FPT_TST_EXT.1: TSF Testing	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM.1(a): Cryptographic Key Generation (Asymmetric Keys)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_COP.1(a): Cryptographic Operation (Signature Verification)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_COP.1(b): Cryptographic Operation (Hash Algorithm)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_COP.1(c): Cryptographic Operation (Keyed Hash Algorithm)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_COP.1(d): Cryptographic Operation (Key Wrapping)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_COP.1(e): Cryptographic Operation (Key Transport)	PP Evaluation
	FCS_COP.1(f): Cryptographic Operation (AES Data Encryption/Decryption)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_COP.1(g): Cryptographic Operation (Key Encryption)	PP Evaluation
	FCS_KDF_EXT.1: Cryptographic Key Derivation	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_PCC_EXT.1: Cryptographic Password Construct and Conditioning	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer

	FCS_RBG_EXT.1: Cryptographic Operation (Random Bit Generation)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_SMC_EXT.1: Submask Combining	PP Evaluation
	FCS_VAL_EXT.1: Validation	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer

6 Assurance Requirements

The following are the assurance requirements contained in the FDEAAcPP.

Table 9: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	ASE_ECD.1: Extended Components Definition	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	ASE_INT.1: ST Introduction	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	ASE_OBJ.1: Security Objectives for the Operational Environment	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	ASE_REQ.1: Stated Security Requirements	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	ASE_SPD.1: Security Problem Definition	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	ASE_TSS.1: TOE Summary Specification	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
ADV: Development	ADV_FSP.1 Basic Functional Specification	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	AGD_PRE.1: Preparative Procedures	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer

	ALC_CMS.1: TOE CM Coverage	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
ATE: Tests	ATE_IND.1: Independent Testing - conformance	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer

7 Results of the Evaluation

Note that for APE elements and work units that are identical to ASE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 10: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer; PP evaluation
APE_ECD.1	Pass	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer; PP evaluation
APE_INT.1	Pass	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer; PP evaluation
APE_OBJ.1	Pass	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer; PP evaluation
APE_REQ.1	Pass	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer; PP evaluation
APE_SPD.1	Pass	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer; PP evaluation

8 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 as interpreted by the supplemental guidance in the FDEAAcPP Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **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.

9 Bibliography

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

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

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] Curtis-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer (FDEEEcPP20/FDEAAcPP20) Security Target, Version 0.6, 18 October 2018.

[7] Assurance Activity Report (FDEEEcPP20/FDEAAcPP20) for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer, Version 0.3, 18 October 2018.

[8] *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0, 9 September 2016.

[9] *collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition*, Version 2.0 + Errata 20190201, 01 February 2019.