Mapping Between

collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019

and

NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 1, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context**. Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **SC-28/SC-28(1).** The purpose of the cPP is to describe the security functionality for supporting the authentication mechanism for encrypted storage. Specifically, the primary security enforcing mechanisms are ensuring that the actual key used to encrypt and decrypt data is inaccessible at rest by unauthorized subjects and is appropriately unlocked for use when the required authorization factor or factors are provided to access it. A TOE that conforms to this PP will provide peripheral support to SC-28 and SC-28(1) by ensuring that data at rest protected by an Encryption Engine cannot be accessed without valid authorization. Many SFRs in this PP are low-level in nature, but their overall effect is to provide peripheral support to the enforcement of SC-28 and SC-28(1).
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to require re-authentication in order to transition out of a compliant power saving state only supports IA-11 to the extent that this behavior falls under the "organization-defined circumstances or situations requiring re-authentication" assigned by that control. The security control assessor must compare the TOE's functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported. In general, the various ancillary security functions that a conformant TOE includes are subordinate to the primary use case of the TOE, which is to ensure that SC-28 and SC-28(1) are enforced to secure data at rest on the organizational asset for which the TOE maintains the decryption key.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
Mandatory Requirements				
FCS_AFA_EXT.1	**Authorization Factor Acquisition**	N/A	**N/A**	The FCS_AFA_EXT.1 SFR does not map to any SP800-53 controls.
FCS_AFA_EXT.2	**Timing of Authorization Factor Acquisition**	N/A	**N/A**	The FCS_AFA_EXT.2 SFR does not map to any SP800-53 controls.
FCS_CKM.4(a)	**Cryptographic Key Destruction (Power Management)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to destroy keys and key material based on organizational policy. The organizational requirements for destruction supported by this SFR is not the algorithm or standard used for destruction, but the timing of when transitioning to a compliant power saving state.
FCS_CKM.4(d)	**Cryptographic Key Destruction (Software TOE, 3rd Party Storage)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_CKM_EXT.4(a)	**Cryptographic Key and Key Material Destruction (Destruction Timing)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to destroy keys when appropriate in order to conform to organizational policy. The organizational

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				requirements for destruction supported by this SFR is not the algorithm or standard used for destruction, but the timing of when keys and key material when no longer needed.
FCS_CKM_EXT.4(b)	**Cryptographic Key and Key Material Destruction (Power Management)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to destroy keys based on organization policy. The organizational requirements for destruction supported by this SFR is not the algorithm or standard used for destruction, but the timing of when transitioning to a compliant power saving state.
FCS_KYC_EXT.1	**Key Chaining (Initiator)**	IA-5	**Authenticator Management**	A conformant TOE protects the authenticator content from unauthorized disclosure and modification by maintaining a key chain, which supports part (g) of the control.
FCS_SNI_EXT.1	**Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of salts, nonces, and/or IVs as needed ensures that cryptographic

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				keys are generated appropriately.
FMT_MOF.1	**Management of Functions Behavior**	AC-6(1)	**Least Privilege:** Authorized Users	A conformant TOE enforces this control on the ability to manage the TOE's power saving state by ensuring that only authorized users may modify the behavior of this.
FMT_SMF.1	**Specification of Management Functions**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional capabilities defined in this SFR. In general, a conformant TOE will satisfy this control to the extent that the TOE provides a method to configure its behavior in accordance with organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE.
FMT_SMR.1	**Security Roles**	AC-6(1)	**Least Privilege:** Authorized Users	A conformant TOE supports the enforcement of least privilege by ensuring that only authorized users are given

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				access to security functions.
FPT_KYP_EXT.1	**Protection of Key and Key Material**	IA-5	**Authenticator Management**	A conformant TOE has the ability to protect key data that may be used an authenticator, satisfying part (g) of the control.
		IA-5(7)	**Authenticator Management:** No Embedded Unencrypted Static Authenticators	A conformant TOE ensures that key data (including authenticators for file system access and any keys that can be used to derive them) are not placed in unencrypted static locations.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will ensure that secret key and keying material data are not stored in plaintext except in specific cases where appropriate.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE will ensure that its cryptographic keys are protected at rest using an appropriate method.
FPT_PWR_EXT.1	**Power Saving States**	N/A	N/A	While the TOE will perform cryptographic operations to

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				secure data at rest when certain power state transitions occur, this SFR only pertains to the definition of the power states themselves and therefore does not address any security controls on its own.
FPT_PWR_EXT.2	**Timing of Power Saving States**	N/A	N/A	While the TOE will perform cryptographic operations to secure data at rest when certain power state transitions occur, this SFR only pertains to when power state transitions occur and therefore does not address any security controls on its own.
FPT_TUD_EXT.1	**Trusted Update**	CM-14	**Signed Components**	A conformant TOE has the ability to require a signed update by the manufacturer prior to installing those updates.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to it.
Optional Requirements				
FPT_TST_EXT.1	**TSF Testing**	SI-6	**Security and Privacy Function Verification**	A conformant TOE will run

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				automatic tests to ensure correct operation of its own functionality.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE has the ability to perform an integrity test of its own software or firmware.
Selection-Based Requirements				
FCS_CKM.1(a)	**Cryptographic Key Generation (Asymmetric Keys)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	The TOE will implement the key generation function using asymmetric keys.
FCS_CKM.1(b)	**Cryptographic Key Generation (Symmetric Keys)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function in support of the key lifecycle process.
		SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	The TOE will implement the key generation function using symmetric keys.
FCS_COP.1(a)	**Cryptographic Operation (Signature Verification)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform signature verification using NSA-approved and FIPS-validated algorithms.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FCS_COP.1(b)	**Cryptographic Operation (Hash Algorithm)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform hashing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(c)	**Cryptographic Operation (Keyed Hash Algorithm)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform keyed-hash message authentication using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(d)	**Cryptographic Operation (Key Wrapping)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key wrapping using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(e)	**Cryptographic Operation (Key Transport)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key transport using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(f)	**Cryptographic Operation (AES Data Encryption / Decryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform AES encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(g)	**Cryptographic Operation (Key Encryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				key encryption using NSA-approved and FIPS-validated algorithms.
FCS_KDF_EXT.1	**Cryptographic Key Derivation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to derive keys in support of the key lifecycle process.
FCS_PCC_EXT.1	**Cryptographic Password Construct and Conditioning**	IA-5(1)	**Authenticator Management:** Password-Based Authentication	A compliant TOE has the ability to condition stored passwords, which satisfies part (c) of this control.
		SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform password-based key derivation based on FIPS- and NSA-approved standards.
FCS_RBG_EXT.1	**Cryptographic Operation (Random Bit Generation)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of an appropriate DRBG ensures that generated keys provide an appropriate level of security.
FCS_SMC_EXT.1	**Submask Combining**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to perform submask combining in support of key generation functions.
FCS_VAL_EXT.1	**Validation**	IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE will ensure that encrypted data at rest is not

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				decrypted unless a valid authorization factor is provided.
		IA-5(7)	**Authenticator Management:** No Embedded Unencrypted Static Authenticators	A conformant TOE supports the enforcement of this control by ensuring that the authorization factors used to validate a user are not persistently stored in an insecure location and subject to unauthorized disclosure.