Mapping Between
collaborative Protection Profile for Full Drive Encryption– Authorization Acquisition, Version 2.0, 09-September-2016
and
NIST SP 800-53 Revision 4

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 4, 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.
- **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 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.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 4 Control**		**Comments and Observations**
FCS_AFA_EXT.1	**<u>Authorization Factor Acquisition</u>**	IA-5	**Authenticator Management**	A conformant TOE will have the ability to ensure that authorization factors are sufficiently strong for use.
		SC-28	**Protection of Information at Rest**	A conformant TOE will ensure the confidentiality of data at rest by requiring the presentation of at least one valid authorization

				factor in order to decrypt stored data.
FCS_AFA_EXT.2	**Timing of Authorization Factor Acquisition**	IA-11	**Re-authentication**	A conformant TOE will require a user to re-authenticate following any transition out of a Compliant power saving state.
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 based on organizational policy and standards.
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 and standards.
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 and standards.
FCS_KYC_EXT.1	**Key Chaining (Initiator)**	SC-13	**Cryptographic Protection**	If the TSF provides the mechanism for securing keys stored in a key chain, it will implement NSA-approved and FIPS-validated cryptography in order to satisfy this function.
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 generated cryptographic keys
FMT_MOF.1	**Management of Functions Behavior**	AC-6	**Least Privilege**	A conformant TOE will enforce least privilege by ensuring that only authorized administrators have the

				ability to manage power saving states.
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 STIGs or other organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE; the security control assessor must review what has been selected in the Security Target and determine what additional support is provided, if any.
		IA-5	**Authenticator Management**	The management functionality of the TSF supports this control by providing the ability for a user to change an authorization factor.
		MP-6	**Media Sanitization**	The management functionality of the TSF supports this control by providing a method to sanitize an encrypted drive by forwarding requests to erase a DEK.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	The management functionality of the TSF supports this control by providing a method to change the value of the DEK that is used to encrypt stored data.
FPT_KYP_EXT.1	**Protection of Key and Key Material**	IA-5	**Authenticator Management**	A conformant TOE has the ability to protect authenticators using PKI.

		SC-12	**Cryptographic Protection**	A conformant TOE will ensure that secret key and keying material data are not stored in plaintext except in specific cases where appropriate.
FPT_PWR_EXT.1	**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 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-5(3)	**Access Restrictions for Change:** Signed Components	A conformant TOE has the ability to require a signed update.
		SI-2	**Flaw Remediation**	A conformant TOE has the ability to remedy implementation flaws through software updates.
		SI-7(1)	**Software, Firmware and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of updates to itself.
Optional Requirements				
FPT_TST_EXT.1	**TSF Testing**	SI-6	**Security Function Verification**	A conformant TOE will run automatic tests to ensure correct operation of its own functionality.

		SI-7	**Software, Firmware, and Information Integrity**	One of the self-tests the TOE may perform is an integrity test of its own software and/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 in support of the key lifecycle process.
		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.
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:** Message Authentication	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 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 has the ability to perform random bit generation based on FIPS and NSA-approved standards.
FCS_SMC_EXT.1	**Submask Combining**	SC-12	**Cryptographic Key Establishment**	A conformant TOE has the ability to perform submask combining in

			and Management	support of key generation functions.
FCS_VAL_EXT.1	**Validation**	AC-3	**Access Enforcement**	A conformant TOE will ensure that encrypted data at rest is not decrypted unless a valid authorization factor is provided.
		SC-28	**Protection of Information at Rest**	A conformant TOE will ensure that information at rest is protected by requiring a valid authorization factor in order to provide access to it.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	The authorization factor used to access protected information at rest is validated using a cryptographic method.