Mapping Between

collaborative Protection Profile for Full Drive Encryption – Encryption Engine, 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 perform self-testing only supports SI-6 to the extent that performing self-tests at initial startup (as defined by FPT_TST_EXT.1.1) is consistent with the verification conditions assigned by part b of the 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_CKM.1(c)	**Cryptographic Key Generation:** Data Encryption Key	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_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_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 Management:** Cryptographic Key and Material Destruction	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to destroy keys based on organization policy and standards.
FCS_CKM_EXT.6	**Cryptographic Key Destruction Types**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will perform key destruction using an appropriate method.
FCS_KYC_EXT.2	**Key Chaining (Recipient)**	SC-12	**Cryptographic Key Establishment and Management**	The ability of a conformant TOE to maintain a key chain satisfies the key access portion of this control.
FCS_SNI_EXT.1	**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 have sufficient strength.
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:**	The authorization factor used to access protected information at rest is validated

			Cryptographic Protection	using a cryptographic method.
FDP_DSK_EXT.1	**Protection of Data on Disk**	AC-19(5)	**Access Control for Mobile Devices:** Full Device/ Container-Based Encryption	If deployed in a mobile device, a conformant TOE has the ability to ensure that the data on that device is protected using full drive encryption.
		SC-28	**Protection of Information at Rest**	The primary purpose of the TOE is to ensure that data at rest is protected against unauthorized access.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE will encrypt data at rest using AES.
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.
		MP-6	**Media Sanitization**	The management functionality of the TSF supports this control by providing a method to sanitize an encrypted

				drive by erasing 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.
		SI-2	**Flaw Remediation**	The management functionality of the TSF supports part c of this control by providing an interface to install software/firmware updates to the TOE.
FPT_KYP_EXT.1	**Protection of Key and Key Material**	IA-5	**Authenticator Management**	A conformant TOE has the ability to ensure the security of key data that may be used as an authenticator to the information that is protected by the TSF.
		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_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.
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_FAC_EXT.1	**Firmware Access Control**	AC-3	**Access Enforcement**	A conformant TOE will not permit application of a firmware update unless proper authorization is provided.
		SI-2	**Flaw Remediation**	A conformant TOE will provide a firmware update mechanism as a remediation method for any flaws found in its implementation.
FPT_RBP_EXT.1	**Rollback Protection**	N/A	N/A	There are no security controls related to the prevention of a software/firmware downgrade operation.
FCS_CKM.4(e)	**Cryptographic Key Destruction:** Key Cryptographic Erase	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to destroy encrypted keys through destruction of a key encryption key.
Selection-Based Requirements				
FCS_CKM.1(a)		SC-12	**Cryptographic Key**	A conformant TOE provides a key

	Cryptographic Key Generation: Asymmetric Keys		**Establishment and Management**	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_CKM.4(b)	**Cryptographic Key Destruction:** TOE-Controlled Hardware	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_CKM.4(c)	**Cryptographic Key Destruction:** General Hardware	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
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_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 encryptionusing 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_RBG_EXT.1	**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 and Management**	A conformant TOE has the ability to perform submask combining in support of key generation functions.
FPT_FUA_EXT.1	**Firmware Update Authentication**	CM-5(3)	**Access Restrictions for**	A conformant TOE has the ability to require a signed update.

			Change: Signed Components	
		SI-2	**Flaw Remediation**	A conformant TOE has the ability to remedy implementation flaws through firmware updates.
		SI-7(1)	**Software, Firmware and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of updates to itself.