Mapping Between collaborative Protection Profile for Dedicated Security Component, Version 1.0, 10 September 2020 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 2, 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.
- **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 enforce access control against protected resources only supports AC-3 to the extent that the TOE's access control functions align with organization-defined access control policies. 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 5 Control		Comments and Observations
Mandatory Requirements				
FCS_CKM.1	**Cryptographic Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate cryptographic keys satisfies the key generation portion of this control.
		SC-12(2) or SC-12(3)	**Cryptographic Key Establishment and Management:** Symmetric Keys -or- **Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE may generate symmetric or asymmetric keys in accordance with applicable standards, depending on the selections made for this requirement.
FCS_CKM.1/KEK	**Cryptographic Key Generation (Key Encryption Key)**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate cryptographic keys satisfies the key generation portion of this control.
		SC-12(2) or SC-12(3)	**Cryptographic Key Establishment and Management:** Symmetric Keys -or- **Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE may generate symmetric or asymmetric keys in accordance with applicable standards, depending on the selections made for this requirement.
FCS_CKM.2	**Cryptographic Key Establishment**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports this control by providing a key establishment function.
		SC-12(3)	**Cryptographic Key Establishment and Management: Asymmetric Keys**	A conformant TOE supports the production of asymmetric keys by providing a key establishment function.
FCS_CKM.4	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys using an appropriate method.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FCS_CKM_EXT.4	**Cryptographic Key and Key Material Destruction Timing**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys in appropriate circumstances.
FCS_COP.1/Hash	**Cryptographic Operation (Hashing)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic hashing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/HMAC	**Cryptographic Operation (Keyed Hash)**	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/KAT	**Cryptographic Operations (Key Agreement/Transport)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key agreement using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/KeyEnc	**Cryptographic Operation (Key Encryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/SigGen	**Cryptographic Operation (Signature Generation)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/SigVer	**Cryptographic Operation (Signature Verification)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/SKC	**Cryptographic Operation (Symmetric Key Cryptography)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_RBG_EXT.1	**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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				appropriate level of security.
FCS_SLT_EXT.1	**Cryptographic Salt Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of salts as needed ensures that generated cryptographic keys have sufficient strength.
FCS_STG_EXT.1	**Protected Storage**	AC-3	**Access Enforcement**	A conformant TOE implements an access control policy that enforces authorized interactions with stored key data.
		AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	The access restrictions enforced by a conformant TOE include restriction of access to cryptographic keys, which is an example of an information type referenced by this control.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Function	A conformant TOE enforces least privilege by identifying the subjects that are authorized to use or destroy key data, such that no other subjects are authorized to perform these operations.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the portion of this control that relates to key storage through this SFR's requirement to implement a protected mechanism for key storage.
		SC-28	**Protection of Information at Rest**	A conformant TOE implements a protected mechanism for key storage.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE implements a protected key storage.
FCS_STG_EXT.2	**Key Storage Encryption**	IA-5(7)	**Authenticator Management:** No Embedded Unencrypted	A conformant TOE supports this control by ensuring that any key data that may be used as an authenticator

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			Static Authenticators	will reside in encrypted storage.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE supports this control by virtue of the fact that the control requires protected storage for cryptographic keys. This SFR requires the TOE to implement a cryptographic method to protect the confidentiality of stored keys.
FCS_STG_EXT.3	**Key Integrity Protection**	SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE supports this control by virtue of the fact that the control requires protected storage for cryptographic keys. This SFR requires the TOE to implement a cryptographic method to protect the integrity of stored keys.
FDP_ACC.1	**Subset Access Control**	AC-3	**Access Enforcement**	A conformant TOE defines an access control policy that governs the operations that subjects can perform against objects protected by the TSF.
FDP_ACF.1	**Security Attribute Based Access Control**	AC-3	**Access Enforcement**	A conformant TOE implements the access control policy defined by FDP_ACC.1.
		AC-3(13)	**Access Enforcement:** Attribute-Based Access Control	A conformant TOE supports this control by implementing attribute-based access control as a mechanism to protect its stored objects.
FDP_ETC_EXT.2	**Propagation of SDOs**	AC-16	**Security and Privacy Attributes**	A conformant TOE ensures any data exported from the TOE is bound with security attributes that associate it with its usage authorizations, satisfying part (a) of the control.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		SC-16	**Transmission of Security and Privacy Attributes**	A conformant TOE supports the enforcement of this control by enforcing conditions on how attribute data is to be exported from the TOE.
FDP_FRS_EXT.1	**Factory Reset**	CP-10	**System Recovery and Reconstitution**	A conformant TOE may support the enforcement of this control by offering a factory reset function that would allow for the TOE to be restored to its original known state.
FDP_ITC_EXT.1	**Parsing of SDEs**	AC-16	**Security and Privacy Attributes**	A conformant TOE ensures any data imported to the TOE is bound with security attributes that associate it with its usage authorizations, satisfying part (a) of the control.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE supports the enforcement of this control by validating the integrity of imported data upon import.
		SC-16	**Transmission of Security and Privacy Attributes**	A conformant TOE supports the enforcement of this control by enforcing conditions on how attribute data is to be imported to the TOE.
FDP_ITC_EXT.2	**Parsing of SDOs**	AC-16	**Security and Privacy Attributes**	A conformant TOE ensures any data imported to the TOE is bound with security attributes that associate it with its usage authorizations, satisfying part (a) of the control.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE supports the enforcement of this control by validating the integrity of imported data upon import.
		SC-16	**Transmission of Security and Privacy Attributes**	A conformant TOE supports the enforcement of this control by enforcing

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				conditions on how attribute data is to be imported to the TOE.
FDP_MFW_EXT.1	**Mutable/Immutable Firmware**	SC-34	**Non-Modifiable Executable Programs**	A conformant TOE may enforce this control by having immutable firmware. If the TOE has mutable firmware, this SFR does not satisfy any controls on its own; rather, it triggers the inclusion of other selection-based SFRs that enforce appropriate protections against mutable firmware
FDP_RIP.1	**Subset Residual Information Protection**	SC-4	**Information in Shared System Resources**	A conformant TOE supports the enforcement of this control by ensuring that protected data does not persist in residual memory for potential unauthorized disclosure.
FDP_SDC_EXT.1	**Confidentiality of SDEs**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	The access restrictions enforced by a conformant TOE include restriction of access to SDEs, which is an example of "selected system information" referenced by this control.
		IA-5	**Authenticator Management**	A conformant TOE supports part (g) of this control for any SDEs that function as authenticator content.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE supports the enforcement of this control by using cryptographic methods to protected stored data at rest.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE supports the enforcement of this control by protecting SDEs that may contain key data.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FDP_SDI.2	**Stored Data Integrity Monitoring and Action**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE monitors stored data for integrity errors.
		SI-7(5)	**Software, Firmware, and Information Integrity:** Automated Response to Integrity Violations	A conformant TOE will automatically react in a specified manner when data integrity violations are detected.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE may implement a cryptographic mechanism to validate the integrity of stored data.
FIA_AFL_EXT.1	**Authorization Failure Handling**	AC-7	**Unsuccessful Logon Attempts**	A conformant TOE supports the enforcement of this control by implementing a mechanism to track successive authorization failures and to enforce a specific reaction is an excessive number of failures is observed.
		AC-7(2)	**Unsuccessful Logon Attempts:** Purge or Wipe Mobile Device	Depending on the selections made in this SFR and the deployment of the TOE, detection of an excessive number of failed authorization attempts may result in the TSF rendering the device in which it resides unusable.
FIA_SOS.2	**TSF Generation of Secrets**	IA-5	**Authenticator Management**	A conformant TOE supports part (c) of this control by ensuring that any authorization data generated by the TSF is sufficiently strong to prevent brute force attacks.
FIA_UAU.2	**User Authentication before Any Action**	AC-14	**Permitted Actions without Identification or Authentication**	A conformant TOE supports the enforcement of this control by ensuring that security-relevant actions

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				cannot be performed against the TSF or protected data without authorization.
FIA_UAU.5	**Multiple Authentication Mechanisms**	IA-2 -or- IA-8	**Identification and Authentication (Organizational Users)** **-or-** **Identification and Authentication (Non-Organizational Users)**	A conformant TOE supports the enforcement of at least one of these controls by providing an authentication mechanism. The specific controls met depend on whether the user is organizational or non-organizational.
FIA_UAU.6	**Re-Authenticating**	IA-11	**Re-Authentication**	A conformant TOE supports the enforcement of this control by requiring subject re-authentication under specific circumstances.
FMT_MOF_EXT.1	**Management of Security Functions Behavior**	AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to manage the TSF.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE associates authorizations to use its security functions with users who belong to authorized roles.
FMT_MSA.1	**Management of Security Attributes**	AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to TSF data to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to manage security attributes of TSF data.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE associates authorizations to use its security functions with users who belong to authorized roles.
		AC-16(2)	**Security and Privacy Attributes:** Attribute Value Changes by Authorized Individuals	A conformant TOE supports the enforcement of this control by ensuring that security attributes of TSF data can only be managed by authorized subjects.
		AC-16(4)	**Security and Privacy Attributes:** Association of Attributes by Authorized Individuals	A conformant TOE supports the enforcement of this control by ensuring that security attributes of TSF data can only be managed by authorized subjects. In particular, the SDO.AuthData attribute of an SDO determines the subjects that are associated with this data and the TSF will restrict the subjects that can modify this attribute to members of an authorized role.
		AC-16(10)	**Security and Privacy Attributes:** Attribute Configuration by Authorized Individuals	A conformant TOE supports the enforcement of this control by ensuring that security attributes of TSF data can only be configured by authorized subjects.
FMT_MSA.3	**Static Attribute Initialization**	CM-6	**Configuration Settings**	A conformant TOE supports the enforcement of this control by defining default settings for the TOE's various security attributes such that the TOE's default security posture is a known state.
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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				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.2	**Restrictions on Security Roles**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE has the ability to associate users with roles, in support of part (a) of the control.
FPT_FLS.1/FI	**Failure with Preservation of Secure State (Fault Injection)**	SC-24	**Fail in Known State**	A conformant TOE supports the enforcement of this control by ensuring that fault injunction attempts will cause the TOE to fail into a known secure state.
FPT_MOD_EXT.1	**Debug Modes**	CM-6	**Configuration Settings**	A conformant TOE supports the enforcement of part (a) of this control by ensuring that the TSF does not have any less-restrictive operational modes that can be entered as a means of bypassing security restrictions.
FPT_PHP.3	**Resistance to Physical Attack**	PE-3(5)	**Physical Access Control:** Tamper Protection	A conformant TOE supports the enforcement of this control by enforcing tamper protection mechanisms on its physical boundary.
FPT_PRO_EXT.1	**Root of Trust**	AC-16	**Security and Privacy Attributes**	A conformant TOE enforces this control by implementing Root of Trust functionality for data stored or generated by the TSF.
FPT_ROT_EXT.1	**Root of Trust Services**	AC-16	**Security and Privacy Attributes**	A conformant TOE enforces this control by implementing Root of Trust functionality for data

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				stored or generated by the TSF.
FPT_ROT_EXT.2	**Root of Trust for Storage**	AC-16	**Security and Privacy Attributes**	A conformant TOE enforces this control by implementing Root of Trust functionality for data stored or generated by the TSF.
FPT_RPL_EXT.1	**Replay Prevention**	IA-2(8)	**Identification and Authentication (Organizational Users):** Access to Accounts – Replay Resistant	A conformant TOE supports the enforcement of this control in the context of I&A by ensuring that authorizations to manipulate TSF data are not subject to replay such that an unauthorized subject could impersonate an authorized one to access this data.
FPT_STM.1	**Reliable Time Stamps**	AU-8	**Time Stamps**	A conformant TOE supports the enforcement of this control by ensuring that the TSF maintains an accurate system clock. Note that this control specifically relates to time stamps in the context of audit records. The PP does not specify FAU_GEN.1 so the TOE's use of time stamps is for non-audit purposes. However, a larger system that includes the TOE as one component may rely on the TOE's system clock when generating its own audit records.
FPT_TST.1	**TSF Testing**	SI-6	**Security and Privacy Function Verification**	A conformant TOE supports part (a) of this control by ensuring the correctness of the TSF through integrity verification.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE supports part (a) of this control by implementing a mechanism

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				to validate the integrity of itself and its stored data.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE supports the enforcement of this control by implementing an integrity check mechanism and defining the circumstances that cause this check to be performed.
FRU_FLT.1	**Degraded Fault Tolerance**	SC-24	**Fail in Known State**	A conformant TOE supports the enforcement of this control by ensuring that fault injunction attempts will cause the TOE to fail into a known secure state.
Optional Requirements				
FCS_ENT_EXT.1	**Entropy for External IT Entities**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's supports the broader organization's enforcement of this control by providing entropy services to external entities so that they can generate strong random numbers.
FCS_RBG_EXT.2	**External Seeding for Random Bit Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's supports the broader organization's enforcement of this control by providing DRBG seeding services to external entities so that they can generate strong random numbers.
FPT_ITT.1	**Basic Internal TSF Data Transfer Protection**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the enforcement of this control by implementing a trusted communications channel for data transmitted between distributed TOE components.
FPT_PRO_EXT.2	**Data Integrity Measurements**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE enforces this control by implementing Root of Trust functionality to maintain the integrity of TSF data.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FPT_ROT_EXT.3	**Root of Trust for Reporting Mechanisms**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE enforces this control by implementing Root of Trust functionality for attesting that the TSF is in a known state.
Selection-Based Requirements				
FCS_CKM.1/AK	**Cryptographic Key Generation (Asymmetric Keys)**	SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	The ability of the TOE to generate cryptographic keys satisfies the key generation portion of this control.
FCS_CKM.1/SK	**Cryptographic Key Generation (Symmetric Encryption Key)**	SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	The ability of the TOE to generate cryptographic keys satisfies the key generation portion of this control.
FCS_CKM_EXT.5	**Cryptographic Key Derivation**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key derivation using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/PBKDF	**Cryptographic Operation (Password-Based Key Derivation Functions)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key derivation using NSA-approved and FIPS-validated algorithms.
FDP_DAU.1/Prove	**Basic Data Authentication (for Use with the Prove Service)**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE supports the enforcement of this control by having the ability to generate the validity of its stored data.
FDP_FRS_EXT.2	**Factory Reset Behavior**	CP-10	**System Recovery and Reconstitution**	A conformant TOE supports the enforcement of this control by having the ability to revert itself to a known factory state.
FDP_MFW_EXT.2	**Basic Firmware Integrity**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE supports the enforcement of part (a) of this control by implementing an integrity check mechanism for TOE firmware.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FDP_MFW_EXT.3	**Firmware Authentication with Identity of Guarantor**	CM-14	**Signed Components**	A conformant TOE supports the enforcement of this control by implementing a mechanism to validate the authenticity of firmware updates using digital signatures.
FIA_AFL_EXT.2	**Authorization Failure Response**	AC-7	**Unsuccessful Logon Attempts**	A conformant TOE supports the enforcement of this control by prevent a bypass of the authentication failure count mechanism.
FPT_FLS.1/FW	**Failure with Preservation of Secure State (Firmware)**	SC-24	**Fail in Known State**	A conformant TOE supports the enforcement of this control by ensuring that attempted loading of invalid firmware will cause the TOE to fail into a known secure state.
FPT_RPL.1/Rollback	**Replay Detection (Rollback)**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE ensures that the integrity of the TSF is maintained by preventing firmware rollbacks to potentially insecure versions.
FTP_CCMP_EXT.1	**CCM Protocol**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements functionality to protect data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE uses a cryptographic protocol to protect data in transit.
FTP_GCMP_EXT.1	**GCM Mode Protocol**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements functionality to protect data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE uses a cryptographic protocol to protect data in transit.
FTP_ITC_EXT.1	**Cryptographically Protected**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements functionality to protect data in transit.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
	Communications Channels	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE uses a cryptographic protocol to protect data in transit.
FTP_ITE_EXT.1	**Encrypted Data Communications**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements functionality to protect data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE protects data in transit by encrypting it prior to transmission such that only the intended recipient can decrypt it.
FTP_ITP_EXT.1	**Physically Protected Channel**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements functionality to protect data in transit.
Objective Requirements				
This PP has no objective requirements.				