Mapping Between Protection Profile for General Purpose Operating Systems, Version 4.2.1, 22-April-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 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 generate audit records only supports AU-2 to the extent that the TOE's audit records are included in the set of "organization-defined auditable events" 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 5 Control		Comments and Observations
Mandatory Requirements				
FCS_CKM.1	**Cryptographic Key Management:** Cryptographic Key Generation	SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE has the ability to generate asymmetric cryptographic keys that use NSA-approved and FIPS-validated cryptographic algorithms. This control satisfies this SFR with respect to key generation.
FCS_CKM.2	**Cryptographic Key Management:** Cryptographic Key Establishment	SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE has the ability to perform key establishment for asymmetric cryptographic keys that use NSA-approved and FIPS-validated cryptographic algorithms. This control satisfies this SFR with respect to key generation.
FCS_CKM_EXT.4	**Cryptographic Key Destruction**	IA-5	**Authenticator Management**	A conformant TOE has the ability to destroy cryptographic keys and plaintext keying material such as passwords to protect authenticator content from unauthorized disclosure and modification.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_COP.1(1)	**Cryptographic Key Operation: Encryption/Decryption**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(2)	**Cryptographic Key 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(3)	**Cryptographic Key Operation: Signing**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(4)	**Cryptographic Key Operation: Keyed-Hash 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_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 appropriate level of security.
FCS_STO_EXT.1	**Storage of Sensitive Data**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to repositories containing credential and key data.
		IA-5(1)	**Authenticator Management:** Password-Based Authentication	Cryptographic security of password data allows for proper enforcement of password-based authentication.
		IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	Cryptographic security of PKI data allows for proper enforcement of public key-based authentication.
		SC-13	**Cryptographic Protection**	The ability of a conformant TOE to encrypt data stored in non-volatile memory ensures the integrity and authenticity of this data.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE has the ability to implement cryptographic mechanisms to prevent unauthorized disclosure and modification of data.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE has the ability to securely store cryptographic keys.
FCS_TLSC_EXT.1	**TLS Client Protocol**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications,

				satisfying this control.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The ability of a conformant TOE to implement TLS 1.2 with a range of mandatory and optional ciphersuites ensures the confidentiality and integrity of data and transit.
		SC-11	**Trusted Path**	If TLS is used to establish a trusted path from the remote administrator to the TSF, a conformant TOE may satisfy this control.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	The TOE supports mutual authentication using X.509v3 certificates.
		SC-13	**Cryptographic Protection**	A conformant TOE's use of TLS to secure data in transit allows it to conform with NSA standards.
FDP_ACF_EXT.1	**Access Controls for Protecting User Data**	AC-3(4)	**Access Enforcement:** Discretionary Access Control	A conformant TOE has the ability to restrict users from accessing resources owned by other users without permission. This control is satisfied because either a DAC or an RBAC privilege model can be used to enforce this.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE has the ability to restrict users from accessing resources owned by other users without permission. control is satisfied ADAC or an RBAC privilege model can be used to enforce this.
FMT_MOF_EXT.1	**Management of Security Functions Behavior**	AC-2(5)	**Account Management:** Inactivity Logout	If optional functionality for configuration of screen lock and/or remote connection inactivity timeout, a conformant TOE has the ability to enforce inactivity logout mechanisms.
		AC-3(7)	**Access Enforcement:** Role-Based Access	This allows a conformant TOE to distinguish between user and

	Control	administrator roles in terms of the level of system access that is available to each.
AC-14	**Permitted Actions without Identification or Authentication**	The ability of a conformant TOE to configure the unauthenticated services that are available to it allows for the implementation of an access control policy.
AC-17	**Remote Access**	If optional functionality for configuration of a remote management server is selected, a conformant TOE has the ability to implement remote access in accordance with an organizational policy.
AU-4	**Audit Log Storage Capacity**	If optional functionality for configuration of audit storage capacity is selected, a conformant TOE will have the ability to satisfy this control.
AU-4(1)	**Audit Log Storage Capacity:** Transfer to Alternate Storage	If optional functionality for configuration of remote audit/logging server is selected, a conformant TOE has the ability to offload audit data to alternate storage.
AU-9(4)	**Protection of Audit Information:** Access by Subset of Privileged Users	This will allow a conformant TOE to assign responsibilities for management of the audit data.
AU-12	**Audit Record Generation**	If optional functionality for configuration of audit rules is selected, a conformant TOE satisfies the control related to the ability to select the events audited by the system.
IA-4	**Identifier Management**	If the optional management function for directory server configuration is selected, a conformant TOE has the ability to support identifier management through connection to a centralized directory

				server.
		IA-5(1)	**Authenticator Management:** Password-Based Authentication	If optional management functions for the composition of user/administrator passwords are selected, a conformant TOE has mechanisms used to ensure strength of secrets for passwords. This satisfies part (h) of the control at a general level but note that the PP only defines rudimentary length and character composition restrictions.
		SC-7	**Boundary Protection**	If optional management functionality for enabling/disabling use of external interfaces is selected, a conformant TOE has the ability to ensure that connectivity to it occurs only through managed and monitored interfaces.
		SC-7(12)	**Boundary Protection:** Host-Based Protection	If optional management functionality for the configuration of a host-based firewall is selected, a conformant TOE has the ability to apply host-based protection to itself.
		SC-7(14)	**Boundary Protection:** Protect Against Unauthorized Physical Connections	If optional management functionality for the ability to enable/disable use of USB ports is selected, a conformant TOE has the ability to restrict physical access to the information system.
		SC-45(1)	**System Time Synchronization:** Synchronization with Authoritative Time Source	If optional functionality for configuration of network time server is selected, a conformant TOE has the ability to satisfy this control.
		SI-2(5)	**Flaw Remediation:** Automatic Software and Firmware Updates	If optional management functionality for configuration of automatic updates is selected, a conformant TOE has the ability to apply automatic updates in accordance with this

				control.
FMT_SMF_EXT.1	**Specification of Management Functions**	AC-2(5)	**Account Management:** Inactivity Logout	If optional functionality for configuration of screen lock and/or remote connection inactivity timeout is selected, a conformant TOE has the ability to enforce inactivity logout mechanisms.
		AC-7	**Unsuccessful Logon Attempts**	A conformant TOE has the ability for an administrator to define a defined number of unsuccessful authentication attempts and take some action when this number is exceeded.
		AC-11	**Device Lock**	A compliant TOE supports this control by requiring user re-authentication following a TSF initiated lock or user initiated lock condition.
		AC-12	**Session Termination**	A compliant TOE supports this control by automatically terminating a user session by an administrator configured time out session of user activity.
		AC-18	**Wireless Access**	If the optional management function of configure WiFi or Bluetooth interface is selected, A conformant TOE will permit an administrator to establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access.
		AU-2	**Event Logging**	If the optional management function configure audit rules is selected, a conformant TOE will permit an administrator to identify the types of events that the system is capable of logging.

		IA-4	**Identifier Management**	If the optional management function for directory server configuration is selected, a conformant TOE has the ability to support identifier management through connection to a centralized directory server.
		IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE will have the ability to enforce some minimum password complexity requirements, although they are not identical to CNSS or DoD requirements or to those specified in part (f) and (h) of this control.
		SC-7(12)	**Boundary Protection:** Host-Based Protection	If optional management functionality for the configuration of a host-based firewall is selected, a conformant TOE has the ability to apply host-based protection to itself.
		SI-2(5)	**Flaw Remediation:** Automatic Software and Firmware updates	If the optional management functionality enable/disable automatic software updates is selected, a conformant TOE may be configured to carry out automatic updates.
FPT_ACF_EXT.1	**Access Controls**	AC-3(4)	**Access Enforcement:** Discretionary Access Control	The TOE has the ability to enforce DAC through enforcement of an access control policy that allows the owner of an object to deny all other subjects access to that object.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	The TOE has the ability to enforce RBAC because the SFR is defining functionality that is unavailable to all users who belong to a particular role.
		AC-6(10)	**Least Privilege:** Prohibit Non-Privileged Users From Executing Privileged Functions	A conformant TOE prohibits unprivileged users from modifying the security settings.

FPT_ASLR_EXT.1	**Address Space Layout Randomization**	SI-16	**Memory Protection**	A conformant TOE has the ability to implement ASLR to prevent unauthorized code execution.
FPT_SBOP_EXT.1	**Stack Buffer Overflow Protection**	SI-16	**Memory Protection**	A conformant TOE has the ability to prevent unauthorized code execution.
FPT_TST_EXT.1	**Boot Integrity**	SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of the boot chain prior to execution.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE has the ability to implement cryptographic mechanisms to detect unauthorized change.
		SI-7(9)	**Software, Firmware, and Information Integrity:** Verify Boot Process	A conformant TOE has the ability to verify the integrity of the boot process.
FPT_TUD_EXT.1	**Trusted Update**	CM-14	**Signed Components**	A conformant TOE has the ability to require a signed update.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of updates to itself.
FPT_TUD_EXT.2	**Trusted Update for Application Software**	CM-14	**Signed Components**	A conformant TOE has the ability to require a signed update.
FAU_GEN.1	**Audit Data Generation**	AC-7	**Unsuccessful Logon Attempts**	The TOE will conform to this control to the extent that it records all unsuccessful logon attempts.
		AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events.
		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data.
		AU-12	**Audit Record Generation**	The TOE has the ability to generate audit logs, as well as control which events are logged, satisfying this control.
FIA_AFL.1	**Authentication Failure Handling**	AC-7	**Unsuccessful Logon Attempts**	The TOE has the ability to detect when a

				defined number of unsuccessful authentication attempts occur and take some corrective action.
FIA_UAU.5	**Multiple Authentication Mechanisms**	IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE can implement one or more methods of authentication for users and administrators.
		IA-2(12)	**Identification and Authentication (Organizational Users):** Acceptance of PIV Credentials	A conformant TOE may support authentication using a PIN that unlocks an asymmetric key. This may potentially be derived from a PIV credential.
		IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE may support password-based authentication, in which case this control would be satisfied.
		IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE may support PKI-based authentication, in which case this control would be satisfied.
FIA_X509_EXT.1	**X.509 Certificate Validation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to certificate path and status, which satisfies this control.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	A conformant TOE specifies what CA's are allowed.
FIA_X509_EXT.2	**X.509 Certificate Authentication**	IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE has the ability to identify and authenticate organizational users using X.509 certificates.
		IA-3	**Device Identification and Authentication**	A conformant TOE as the ability to identify and authenticate itself to trusted remote entities using mutual authentication.
FTP_ITC_EXT.1	**Trusted Channel Communication**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	The use of the cryptographic protocols specified in the SFR implies that the TOE can perform mutual authentication with trusted remote entities.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic	The use of the protocols specified in the SFR ensures the confidentiality and

			Protection	integrity of information transmitted between the TOE and another trusted IT product.
FTP_TRP.1	**Trusted Path**	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE will have the ability to prevent unauthorized disclosure of information and also detect modification to that information.
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself.
Optional Requirements				
FCS_TLSC_EXT.4	**TLS Client Protocol**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	The use of mutual X.509 certificate authentication allows a conformant TOE to perform cryptographic bidirectional authentication.
FDP_IFC_EXT.1	**Information Flow Control**	AC-4	**Information Flow Enforcement**	A conformant TOE has the ability to establish an IPsec channel with remote VPN endpoint and block traffic that doesn't meet the IPsec security policy.
		AC-17	**Remote Access**	A conformant TOE has the ability to establish connections with a remote VPN endpoint and block traffic that doesn't meet the IPsec security policy.
FTA_TAB.1	**Default TOE Access Banners**	AC-8	**System Use Notification**	The TOE displays an advisory warning to the user prior to authentication.
		AC-14	**Permitted Actions Without Identification or Authentication**	A conformant TOE displays an advisory warning to the user prior to authentication.
		PL-4	**Rules of Behavior**	The TOE displays an advisory warning to the user prior to authentication to identify the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy.

Selection-based Requirements				
FCS_DTLS_EXT.1	**DTLS Implementation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications, satisfying this control.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The ability of a conformant TOE to implement DTLS with a range of mandatory and optional ciphersuites ensures the confidentiality and integrity of data and transit.
		SC-11	**Trusted Path**	If DTLS is used to establish a trusted path from the remote administrator to the TSF, a conformant TOE may satisfy this control.
		SC-13	**Cryptographic Protection**	A conformant TOE's use of DTLS to secure data in transit allows it to conform with NSA standards.
FCS_TLSC_EXT.2	**TLS Client Protocol**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to limit the elliptic curves that can be used for key establishment.
Objective Requirements				
FCS_TLSC_EXT.3	**TLS Client Protocol**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to ensure the TLS connection is negotiated within a more restrictive set of acceptable parameters.
FPT_SRP_EXT.1	**Software Restriction Policies**	CM-5(6)	**Access Restrictions for Change:** Limit Library Privileges	To the extent that a conformant TOE has the ability to implement a whitelisting policy defined by the organization, this SFR satisfies this control.
FPT_W^X_EXT.1	**Write XOR Execute Memory Pages**	SI-16	**Memory Protection**	Implementation of this SFR is a method by which a conformant TOE will protect memory from unauthorized code execution.