Mapping Between Protection Profile for General Purpose Operating Systems, Version 4.1, 09-March-2016 and NIST SP 800-53 Revision 4

Introduction

This section outlines the NIST SP 800-53/CNSS 1253 controls that may be addressed by compliant TOEs and can be used by certification personnel to determine what, if any, additional testing is required when the TOE is incorporated into its operational configuration.

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.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 4 Control**		**Comments and Observations**
FCS_CKM.1(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(1)	**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.3	**Cryptographic Key Management:** Cryptographic Key Destruction	SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	A conformant TOE has the ability to perform key destruction in accordance with a defined specification.
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.

		SC-13	**Cryptographic Protection**	A conformant TOE has the ability to generate random bits for use in cryptographic services using FIPS and NSA-approved standards.
FCS_STO_EXT.1	**Storage of Sensitive 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:** PKI-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.
FCS_TLSC_EXT.1	**Transport Layer Security Client Protocol**	IA-5(2)	**Authenticator Management:** PKI-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications, satisfying this control.
		SC-8(1)	**Transmission Integrity:** Cryptographic or Alternate Physical 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-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	**User Data Protection** 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.
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.
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 Control	This allows a conformant TOE to distinguish between user and 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 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 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-8(1)	**Time Stamps:** 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.
		AU-9(4)	**Protection of Audit Information**	This will allow a conformant TOE to assign responsibilities for management of the audit data.
		AU-12	**Audit 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	**Authenticator Management**	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.
		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:** Protects 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.
		SI-2(5)	**Flaw Remediation:** Automatic Software / 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.
FPT_ACF_EXT.1	**Access Controls**	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	**Least Privilege**	A conformant TOE only gives authorized access to users that are required to complete assigned tasks in accordance with organizational missions.
		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:**	A conformant TOE has the ability to implement cryptographic mechanisms to detect

			Cryptographically-validated integrity	unauthorized change.
		SI-7(9)	**Software, Firmware and Information Integrity:** Integrity of system boot	A conformant TOE has the ability to verify the integrity of the boot process.
FPT_TUD_EXT.1	**Integrity for Installation and Update**	CM-5(3)	**Access Restrictions For Change:** 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-5(3)	**Access Restrictions For Change:** Signed Components	A conformant TOE has the ability to require that third-party applications running on it use signed updates.
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	**Auditable Events**	A conformant TOE has the ability to generate audit records for various events.
		AU-3	**Audit Record Contents**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data.
		AU-12	**Audit 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**	IA-2	**Identification and**	A conformant TOE can

	Authentication Mechanisms		**Authentication**	implement one or more methods of authentication for users and administrators.
		IA-2(12)	**Identification and Authentication:** 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:** PKI-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:** PKI-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**	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 or Alternate Physical Protection	The use of the protocols specified in the SFR ensures the confidentiality and 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 For Alternate Physical 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.
ADV_FSP.1	**Basic Functional Specification**	SA-4(1)	**Acquisition Process:** Functional Properties of Security Controls	A conformant TOE will provide a functional specification as part of the Security Target which describes the security functionality of each external interface.
AGD_OPE.1	**Operational User Guidance**	SA-5	**Information System Documentation**	The TOE includes guidance documentation that is reviewed as part of the evaluation includes operational instructions.
AGD_PRE.1	**Preparative Procedures**	SA-5	**Information System Documentation**	The TOE includes guidance documentation that is reviewed as part of this evaluation defines installation and preparation procedures.
ALC_CMC.1	**Life-Cycle Support**	CM-9	**Configuration Management Plan**	The evaluation of a conformant a TOE will demonstrate that it provides a unique identification for itself, which can be used as an input to a comprehensive CM Plan.

		SA-10	**Developer Configuration Management**	The evaluation of a conformant a TOE will demonstrate that it provides a unique identification for itself, which can be used as an input to a developer configuration management system.
ALC_CMS.1	**TOE CM Coverage**	CM-9	**Configuration Management Plan**	The evaluation of a conformant a TOE will demonstrate that it provides a configuration list for its own components, which can be used as an input to a comprehensive CM Plan.
		SA-10	**Development Configuration Management**	The evaluation of a conformant a TOE will demonstrate that it provides a configuration lst for its own components, which can be used as an input to a developer configuration management system.
ALC_TSU_EXT.1	**Timely Security Updates**	MA-6(1)	**Timely Maintenance:** Preventive Maintenance	A conformant TOE includes a description of how timely security updates must be applied for the purpose of preventative maintenance.
ATE_IND.1	**Independent Testing**	CA-2	**Security Assessments**	A conformant TOE will have a security assessment performed against it.
		CA-2(1)	**Security Assessments:** Independent Assessors	A conformant TOE will be evaluated by an independent assessor as part of the evaluation process.
AVA_VAN.1	**Vulnerability Assessment**	CA-2(2)	**Security Assessments:** Specialized Assessments	A conformant TOE will have a vulnerability scan performed against it as a specialized assessment method.

		CA-8	**Penetration Testing**	Penetration testing is performed on a conformant TOE to determine that it is resistant to attacks. satisfying this control.
		RA-3	**Risk Assessment**	As part of the evaluation, a conformant TOE will be tested for its resistance against vulnerabilities that meet a given risk level as determined by the PP authors.
		SA-11(2)	**Developer Security Testing and Evaluation:** Threat And Vulnerability Analyses	The Protection Profile defines threats for a given technology type that a conformant TOE is expected to mitigate. However, the TOE developer may not conduct this assessment prior to independent evaluators.
		SA-11(5)	**Developer Security Testing and Evaluation:** Penetration Testing/ Analysis	The Protection Profile mandates that a conformant TOE be subjected to relevant penetration testing. However, the TOE developer may not conduct this assessment prior to independent evaluators.
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.
FTA_TAB.1	**Default TOE Access Banners**	AC-8	**System Use Notification**	The TOE displays an advisory warning to the user prior to authentication.
Selection-based Requirements				
FCS_DTLS_EXT.1	**DTLS Implementation**	IA-5(2)	**Authenticator Management:**	The TOE requires peers to possess a valid

			PKI-Based Authentication	certificate before establishing trusted communications, satisfying this control.
		SC-8(1)	**Transmission Integrity:** Cryptographic or Alternate Physical 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(7)	**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.