Mapping Between Collaborative Protection Profile for Network Devices, Version 1.0, 27-Feb-2015 and NIST SP 800-53 Revision 4

Introduction

Several of the NIST SP 800-53/CNSS 1253 controls are either fully or partially addressed by compliant TOEs. This section outlines the requirements that are addressed, 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.

5. Security Functional Requirements

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
FAU_GEN.1	**Security Audit Data Generation** Audit Data Generation • Product generates audit records for the following events a) Start-up and shut-down of the audit functions; b) All auditable events for the not specified level of audit; and c) All administrative actions comprising: ●$_1$ Administrative login and logout (name of user account shall be logged if individual user accounts are required for	AC-2(4)	**Account Management** | Automated Audit Actions • Information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*personnel or roles*].	FAU_GEN.1.1 item c ●$_2$ would support satisfaction of AC-2(4), which is also dependent on the completion of the assignment in AU-2.
		AC-3(10)	**Access Enforcement** | Audited Override of Access Control Mechanisms • Organization employs an audited override of automated access control mechanisms under	Depending on the completion of FAU_GEN.1.1 item c ●$_6$, satisfaction of this control may be supported, which is also dependent on the

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
	administrators). ●2 Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed). ●3 Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged). ●4 Resetting passwords (name of related user account shall be logged). ●5 Starting and stopping services (if applicable) ●6 *Selection: [no other actions, assignment: [list of other uses of privileges]]*; d) Specifically defined auditable events listed in Table 1.. • Product records within the audit record at least date, time, type, instigator, outcome, and [*event specific information*]		[*conditions*].	completion of the assignment in AU-2.
		AC-6(9)*	**Least Privilege** | Auditing Use of Privileged Functions • Information system audits the execution of privileged functions.	Depending on the completion of FAU_GEN.1.1 item c ●6, satisfaction of this control may be supported, which is also dependent on the completion of the assignment in AU-2.
		AU-2	**Audit Events** Organization… • Determines system can audit [events] • […] • Determines the following events are to be audited: [events]	FAU_GEN.1.1 supports satisfaction of AU-2, depending on the congruity between the audited actions in FAU_GEN.1.1 and the completed assignment in AU-2. Note also that the list of auditable events in FAU_GEN.1.1 may not be sufficient to address or support all the required audited events in the CNSSI № 1253 completion of AU-2.
		AU-3	**Content of Audit Records** • Information system generates records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event	FAU_GEN.1.2 supports satisfaction of AU-3.
		AU-3(1)	**Content of Audit Records** | Additional Audit Information • Information System generates records containing [*additional information*]	FAU_GEN.1.2 supports satisfaction of AU-3(1), depending on the congruity between the additional information required by FAU_GEN.1.2 and the completed assignment in AU-3(1).
		AU-12	**Audit Generation** Information system… • Provides audit record generation capability for the auditable events defined in AU-2 a. at [*components*]; • Allows [*personnel or roles*] to select which auditable events are to be audited by specific components of the information system • Generates audit records for the events defined in AU-2 d. with the content defined	FAU_GEN.1.1 supports satisfaction of AU-12, depending on the congruity between the audited actions in FAU_GEN.1.1 and the completed assignment in AU-12.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			in AU-3.	
		MA-4(1)	**Nonlocal Maintenance** | Auditing and Review Organization… • Audits nonlocal maintenance and diagnostic sessions [*audit events*]; • Reviews the records of the maintenance and diagnostic sessions.	Depending on the completion of FAU_GEN.1.1 item c ●6, satisfaction of this control may be supported, which is also dependent on the completion of the assignment in AU-2.
		SI-7(8)	**Software, Firmware, and Information Integrity** | Auditing Capability for Significant Events • Information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [*(one or more): generates an audit record; alerts current user; alerts [personnel or roles]; [other actions]*].	Depending on the completion of FAU_GEN.1.1 item c ●6, satisfaction of this control may be supported, which is also dependent on the completion of the assignment in AU-2.
FAU_GEN.2	**Security Audit Data Generation** User Identity Association • Auditable events are associated with the identity of the user that caused the event	AU-3	**Content of Audit Records** • Information system generates records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event	FAU_GEN.2 supports satisfaction of the last clause of AU-3 ("the identity of any individuals or subjects associated with the event").
FAU_STG_EXT.1	**Protected Audit Event Storage** • Product can transmit generated audit data to an external IT entity using a trusted channel • Product can store generated audit data on the TOE itself. • Product [*selection: drop, overwrite according to rule, other*] when the local storage space for audit data is full.	AU-4	**Audit Storage Capacity** • Organization allocates audit record storage in accordance with [*storage requirements*]	With appropriate assignments for local buffers and network storage, AU-4 is supported by this SFR. Note also that this is at a *product* level; at a *system* level, the AU-4 assignment changes to incorporate the remote storage (as it is part of the system, not the product), and AU-4(1) goes away as it refers to off-site storage.
		AU-4(1)	**Audit Storage Capacity** | Transfer to Alternate Storage • Information system off-loads audit records [*frequency*] onto a different system or media than the system being audited.	AU-4(1) is supported at the product level. At a *system* level, the AU-4 assignment changes to incorporate the remote storage (as it is part of the system, not the product), and AU-4(1) goes away as it refers to off-site storage.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
		AU-5	**Response to Audit Processing Failures** Information system… • Alerts [*personnel or roles*] in the event of an audit processing failure • Takes [*additional actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].	The SFR supports AU-6, although it does not alert. Again, the product/system distinction is critical.
FCS_CKM.1	**Cryptographic Key Management** Cryptographic Key Generation • Product generates **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [*selection:* ●1 *RSA schemes…* ●2 *ECC schemes…* ●3 *FFC schemes…*]	SC-12	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	This SFR supports SC-12, under the presumption that SC-12 has been completed with a congruent assignment with respect to key generation.
		SC-12(3)	**Cryptographic Key Establishment and Management** | Asymmetric Keys • Organization produces, controls, and distributes asymmetric cryptographic keys using [*NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key*].	As this SFR is explicitly referencing asymmetric keys, this SFR supports SC-12(1), under the presumption that the SC-12(1) has been completed with a congruent assignment with respect to key generation.
FCS_CKM.2	**Cryptographic Key Management** Cryptographic Key **Establishment** • Product **establishes** cryptographic keys in accordance with [*selection:* ●1 *RSA-based schemes…* ●2 *Elliptic curved-based schemes…* ●3 *Finite Field-based schemes…*].	SC-12	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	This SFR supports SC-12, under the presumption that SC-12 has been completed with a congruent assignment with respect to key establishment.
		SC-12(3)	**Cryptographic Key Establishment and Management** | Asymmetric Keys • Organization produces, controls, and distributes asymmetric cryptographic	As this SFR is explicitly referencing asymmetric keys, this SFR supports SC-12(1), under the presumption that the SC-12(1) has been completed with a

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			keys using [*NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key*].	congruent assignment with respect to key establishment.
FCS_CKM.4	**Cryptographic Key Management** Cryptographic Key Destruction • Product destroys cryptographic keys in accordance with [*selection:* ●1 *for volatile memory…* ●2 *for non-volatile EEPROM…* ●3 *for non-volatile flash memory…* ●4 *for other non-volatile memory…*] that meets the following: [*no standard*].	SC-12	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	As management includes destruction, this SFR supports SC-12, under the presumption that SC-12 has been completed with a congruent assignment with respect to key destruction.
FCS_COP.1(1)	**Cryptographic Operation** Cryptographic Operation (AES Data Encryption/Decryption) • Product performs [*encryption / decryption*] in accordance with [*AES used in …. modes*] and [*cryptographic key sizes*] that meet the following: [*list of ISO standards*].	AC-17(2)	**Remote Access** | Protection of Confidentiality / Integrity Using Encryption • Information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	To the extent AES is used to support remote access encryption, AC-17(2) is supported.
		SC-13	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	FCS_COP.1(1) supports SC-13 to the extent to which the assignments are congruent. **Note:** The security engineer must ensure that use of cryptographic mechanisms is properly integrated into the overall system.
FCS_COP.1(2)	**Cryptographic Operation** Cryptographic Operation (Signature Generation and Verification) • Product performs [*cryptographic signature services*] in accordance with [*RSA DSA, EC DSA*] that meet the following: [*list of ISO standards*].	CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	FCS_COP.1(2) supports this control through the provision of digital signatures.
		AU-10	**Non-Repudiation** • Information system protects against an individual (or process acting on behalf of an individual) falsely	FCS_COP.1(2) supports this control through the provision of digital signatures.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			denying having performed [*actions to be covered by non-repudiation*].	
		SC-13	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	FCS_COP.1(2) supports SC-13 to the extent to which the assignments are congruent. **Note:** The security engineer must ensure that use of cryptographic mechanisms is properly integrated into the overall system.
		SI-7(15)	**Software, Firmware, and Information Integrity** | Code Authentication • Information system implements cryptographic mechanisms to authenticate [*software or firmware components*] prior to installation.	FCS_COP.1(2) supports this control through the provision of digital signatures.
FCS_COP.1(3)	**Cryptographic Operation** Cryptographic Operation (Hash Algorithm) • Product performs [*hasing*] in accordance with [*SHA-1, SHA-256, SHA-384, SHA-512*] that meet the following: [*IISO/IEC 10118-3:2004*].	SC-13	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	FCS_COP.1(3) supports SC-13 to the extent to which the assignments are congruent. **Note:** The security engineer must ensure that use of cryptographic mechanisms is properly integrated into the overall system.
		SI-7(15)	**Software, Firmware, and Information Integrity** | Code Authentication • Information system implements cryptographic mechanisms to authenticate [*software or firmware components*] prior to installation.	FCS_COP.1(3) supports this control through the provision of cryptographic hashes.
FCS_COP.1(4)	**Cryptographic Operation** Cryptographic Operation (Keyed Hash Algorithm) • Product performs [*keyed-hash message authentication*] in accordance with [*HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512*] and [*cryptographic key sizes*] and message digest sizes [*160, 256, 384, 512*] bits that meet the following: [*ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*].	SC-13	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	FCS_COP.1(4) supports SC-13 to the extent to which the assignments are congruent. **Note:** The security engineer must ensure that use of cryptographic mechanisms is properly integrated into the overall system.
FCS_RBG_EXT.1	**Random Bit Generation** Random Bit Generation • Product performs all deterministic random bit generation services in accordance	SC-13	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance	FCS_RBG_EXT.1 supports SC-13 to the extent to which the assignments are congruent. **Note:** The security

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
	with ISO/IEC 18031:2011 using [*methods*]. • Deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [*[number] software-based noise source, [number] hardware-based noise source*] with a minimum of [*number of bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 of the keys and hashes that it will generate.		with applicable federal laws … and standards.	engineer must ensure that use of cryptographic mechanisms is properly integrated into the overall system.
FIA_PMG_EXT.1	**Password Management** Password Management • Product provides the following password management • capabilities for administrative passwords: [*complexity requirements*]	IA-5	**Authenticator Management** Organization manages information system authenticators by… • […] • Establishing initial authenticator content for authenticators defined by the organization • Ensuring that authenticators have sufficient strength of mechanism for their intended use • […]	There is a marginal connection to IA-5, in that a product implementing FIA_SOS assists in implementing item c in IA-5, ensuring that authenticators have sufficient strength. It is important to note, however, that IA-5 can be satisfied through procedural means, whereas FIA_PMG_EXT.1 requires a product capability.
		IA-5(1)	**Authenticator Management** | Password-Based Authentication Information system, for password-based authentication… • Enforces minimum password complexity of [*complexity requirements*]; • Enforces at least the following number of changed characters when new passwords are created: [*number*] • Stores and transmits only encrypted representations of passwords • Enforces password minimum and maximum lifetime restrictions of [*minimum, maximum*]; • Prohibits password reuse for [*number*] generations • Allows the use of a temporary password for system logons with an immediate change to a permanent password.	If the product is implementing a password-based mechanism, than the complexity assignment in FIA_PMG_EXT.1 may be sufficient to address the complexity mechanisms (item a) of IA-5(1). Note that the complexity mechanisms chosen by the product may not be sufficient to meet service requirements; PP authors should consider consulting CNSSI 1253 and the specified assignment for IA-5(1). **Note:** Many of the restrictions of IA-5(1) are not addressed within the context of the CC, other than by extended requirements or a complicated assignment for FIA_PMG_EXT.1. In particular, it is worth noting that the CC has no explicit requirements to ensure passwords are stored in an obscured fashion (hashed or encrypted).

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations

FIA_UIA_EXT.1	**User Identification and Authentication (Extended)**
	User Identification and Authentication
	• Product allows the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:
	  • Display the warning banner in accordance with FTA_TAB.1;
	  • [*other actions, if any*]
	• Product requires each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.
		AC-14	**Permitted Actions without Identification or Authentication**
			Organization…
			• Identifies [*user actions*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions
			• Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.
				FIA_UIA_EXT.1.1 supports identification of the actions for AC-14. AC-14 goes beyond FIA_UAU in that it requires rationale for each permitted action. The assignments must be congruent between FIA_UAU and AC-14.
				Note: FIA_UAU addresses AC-14 only for the particular evaluated product. AC-14 must still be considered in an overall system context.

		IA-2	**Identification and Authentication (Organizational Users)** • Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	FIA_UIA_EXT supports I&A of organizational users. It is presumed that administrators are organizational users; if not, IA-8 may also be supported.
FIA_UAU_EXT.2	**User Identification and Authentication (Extended)** Password-based Authentication Mechanism • Product provides a local password-based authentication mechanism, [*any other mechanisms*] to perform administrative user authentication.	IA-5	**Authenticator Management ‡** Organization manages information system authenticators by… • […] • Establishing initial authenticator content for authenticators defined by the organization • Ensuring that authenticators have sufficient strength of mechanism for their intended use • […]	FIA_UAU_EXT.2 supports IA-5 by requiring local authenticators.
		IA-5(1)	**Authenticator Management** | Password-Based Authentication Information system, for password-based authentication… • Enforces minimum password complexity of [*complexity requirements*]; • Enforces at least the following number of changed characters when new passwords are created: [*number*] • Stores and transmits only encrypted representations of passwords • Enforces password minimum and maximum	FIA_UAU_EXT.2 supports IA-5(1) by requiring local password-based authenticators.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			lifetime restrictions of [*minimum, maximum*]; • Prohibits password reuse for [*number*] generations • Allows the use of a temporary password for system logons with an immediate change to a permanent password.	
		Note: Additional enhancements from IA-2 or IA-5 may be supported, depending on how the assignment is completed.		
FIA_UAU.7	**User Authentication** Protected Authentication Feedback • Product provides only [*list of feedback*] to the user while the authentication is in progress.	IA-6	**Authenticator Feedback** • Information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Presuming that FIA_UAU.7 was completed to require obscured feedback, IA-6 is satisfied at the product level.
FIA_X509_EXT.1	**Authentication using X.509 certificates (Extended – FIA_X509_EXT)** X.509 Certificate Validation • Product validates certificates in accordance with the following rules: …. • Product only treats a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.	IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; • Enforces authorized access to the corresponding private key; • Maps the authenticated identity to the account of the individual or group; • Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	This SFR supports certificate validation. The specific methods of validation are at a level of detail below that in NIST SP 800-53.
FIA_X509_EXT.2	**Authentication using X.509 certificates (Extended – FIA_X509_EXT)** X.509 Certificate Authentication • Product uses X.509v3 certificates as defined by RFC 5280 to support authentication for [*selection: IPsec, TLS, HTTPS, SSH*], and [*selection: code signing for system software updates, code signing for integrity verification, [assignment: other uses], no additional uses*]. • When the product cannot establish a connection to determine the validity of a	IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; • Enforces authorized access to the corresponding private key; • Maps the authenticated identity to the account of	This SFR supports use of certificates for authentication.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
	certificate, it [*selection: allows the administrator to choose whether to accept the certificate in these cases, accepts the certificate, does not accept the certificate*].		the individual or group; • Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	
		AU-10 *conditionally*	**Non-Repudiation** • Information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*actions to be covered by non-repudiation*].	If the assignment is completed to use these certificates for non-repudiation/digital signatures, AU-10 would be supported.
		CM-5(3) *Conditionally*	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	To the extent to which the certificates are used to support code authentication, CM-5(3) is supported.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Authentication for protocol use supports transmission confidentiality.
		SC-11	**Trusted Path** • Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	Authentication for protocol use supports trusted path.
		SI-7(6) *Conditionally*	**Software, Firmware, and Information Integrity** | Cryptographic Protection • Information system implements cryptographic mechanisms to detect unauthorized changes to	To the extent to which the certificates are used to support code authentication, CM-5(3) is supported.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			software, firmware, and information.	
		SI-7(15) *Conditionally*	**Software, Firmware, and Information Integrity** | Code Authentication • Information system implements cryptographic mechanisms to authenticate [*software or firmware components*] prior to installation.	This SFR supports SI-7(15), as one of the mechanisms used are digital signatures and certificates.
FIA_X509_EXT.3	**Authentication using X.509 certificates (Extended – FIA_X509_EXT)** X.509 Certificate Requests • Product generates a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key and [*selection: device-specific information, Common Name, Organization, Organizational Unit, Country*]. • Product validates the chain of certificates from the Root CA upon receiving the CA Certificate Response.	IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; • Enforces authorized access to the corresponding private key; • Maps the authenticated identity to the account of the individual or group; • Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	This SFR supports use of certificates for authentication.
FMT_MOF.1(1)	**Management of Functions in TSF** Management of Security Functions Behavior / Trusted Update • Product restricts the ability to [*enable*] the functions [*perform manual update*] to [*security administrators*].	AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Restriction of management functions to particular roles supports implementation of RBAC.
		AC-6	**Least Privilege** • Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Provision of limited management functionality divided by role supports satisfaction of least privilege. **Note:** Support for the principle of least privilege at a product level does not guarantee it is implemented effectively across the entire system.
FMT_MTD.1	**Management of TSF Data**	AC-3(7)	**Access Enforcement** | Role-Based Access	Restriction of management functions

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
	Management of TSF Data • Product restricts the ability to [*manage*] the [*TSF data*] to [*security administrators*].		Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	to particular roles supports implementation of RBAC.
		AC-6	**Least Privilege** • Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Provision of limited management functionality divided by role supports satisfaction of least privilege. **Note:** Support for the principle of least privilege at a product level does not guarantee it is implemented effectively across the entire system.
		AU-6(7)	**Audit Review, Analysis, and Reporting** | Permitted Actions • Organization specifies the permitted actions for each [*process; role; user*] associated with the review, analysis, and reporting of audit information.	If the TSF data being managed is audit data, this control may be satisfied.
FMT_SMF.1	**Specification of Management Functions** Specification of Management Functions • Product is of performing the following management functions: • Ability to administer the TOE locally and remotely; • Ability to configure the access banner; • Ability to configure the session inactivity time before session termination or locking; • Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates; • [*selection:* • *Ability to configure audit behavior;* • *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;* • *Ability to configure the cryptographic functionality;*	AC-11	**Session Lock** Information system… • Prevents further access to the system by initiating a session lock after [*time period*] of inactivity or upon receiving a request from a user • Retains the session lock until the user reestablishes access using established identification and authentication procedures.	Configuration of session inactivity timer supports session lock.
		AU-12(3)	**Audit Generation** | Changes by Authorized Individuals • Information system provides the capability for [*individuals or roles*] to change the auditing to be performed on [*information system components*] based on [*selectable event criteria*] within [*time thresholds*].	To the extent configuration of audit behavior is supported, AU-12(3) is supported.
		CM-6	**Configuration Settings** Organization… • Establishes and documents configuration settings for information technology products employed within	The ability to configure the product supports implementation of the configuration settings.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
	• *No other capabilities.*].		the information system using [*security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; • Implements the configuration settings; • Identifies, documents, and approves any deviations from established configuration settings for [*information system components*] based on [*operational requirements*]; and • Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	
		IA-7 *Conditionally*	**Cryptographic Module Authentication** • Information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, […] for such authentication.	Configuration of cryptographic functionality would include module authentication.
		Note: For many of these functions, the ability to configure the function is not called out explicitly in 800-53, even though the function may be.		
FMT_SMR.2	**Security Management Roles** Restrictions on Security Roles • Product maintains the roles [*Security Administrator*]. • Product can associate users with roles. • Product ensures that the conditions [*administer locally; administer remotely*] are satisfied.	AC-2(7)	**Account Management** | Role-Based Schemes Organization… • Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles • Monitors privileged role assignments • Takes [*actions*] when privileged role assignments are no longer appropriate.	Requiring the role supports a role-based scheme.
		AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	AC-3(7) supports RBAC by providing the ability to define the roles.
		AC-5	**Separation of Duties**	Arguably, if a system

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			Organization… • Separates [*duties of individuals*] • Documents separation of duties of individuals • Defines information system access authorizations to support separation of duties.	provides distinct roles, that supports the provision of separation of duties and supports item c. of AC-5.
		AC-6	**Least Privilege** • Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	If a system provides distinct roles, that supports the provision of separation of duties and the application of the principle of least privilege.
FPT_SKP_EXT.1	**Protection of TSF Data (Extended – FPT_SKP_EXT)** Protection of TSF Data (for reading of all symmetric keys) • Product prevents reading of all pre-shared keys, symmetric keys and private keys.	IA-5	**Authenticator Management** Organization manages information system authenticators by… • […] • Protecting authenticator content from unauthorized disclosure and modification • […]	This SFR supports protection of stored keys.
		IA-5(6)	**Authenticator Management** | Protection of Authenticators • Organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.	This SFR supports protection of stored keys.
FPT_APW_EXT.1	**Protection of TSF Data** Protection of Administrator Passwords • Product stores password in non-plaintext form • Product prevents the reading of plaintext passwords	IA-5	**Authenticator Management** Organization manages information system authenticators by… • […] • Protecting authenticator content from unauthorized disclosure and modification • […]	This SFR supports protection of stored keys.
		IA-5(1)	**Authenticator Management** | Password-Based Authentication Information system, for password-based authentication… • […] • Stores and transmits only encrypted representations	This SFR supports protection of stored passwords.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			of passwords • […]	
		IA-5(6)	**Authenticator Management** | Protection of Authenticators • Organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.	This SFR supports protection of stored passwords.
		Note: IA-5(7) prohibits use of unencrypted authenticators in access scripts. This is not noted in the cPP SFR, nor is it checked in the authentication activity for FPT_APW_EXT.1.		
FPT_TST_EXT.1	**Protection of TSF Data** TSF testing (Extended) • Product runs a suite of the following self-tests [*selection: during initial start-up (on power on), periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-tests should occur]*] to demonstrate the correct operation of the product: [*list of self-tests run by the product*].	SI-6	**Security Function Verification** Information system… • Verifies the correct operation of [*security functions*]; • Performs this verification [*(one or more): [system transitional states]; upon command by user with appropriate privilege; [frequency]*]; • Notifies [*personnel or roles*] of failed security verification tests; • [*(one or more): shuts the information system down; restarts the information system; [alternative action(s)]*] when anomalies are discovered.	This SFR supports satisfaction of SI-6 for the system, but the system must perform tests for all components in the system that provide security functions.
FPT_TUD_EXT.1	**Trusted Update** Trusted Update • Product provides Security Administrators the ability to query the currently executing version of the TOE firmware/software as well as the most recently installed version of the TOE firmware/software. • Product provides Security Administrators the ability to manually initiate updates to TOE firmware/software and [*selection: support automatic checking for updates, support automatic updates, no other update mechanism*]. • Product provides means to authenticate firmware/software updates to the TOE using a [*selection: digital signature mechanism, published hash*] prior to installing those updates.	CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	FPT_TUD_EXT.1.3 supports CM-5(3)
		CM-8	**Information System Component Inventory** Organization… • Develops and documents an inventory of information system components that: (1) Accurately reflects the current information system; (2) Includes all components within the authorization boundary of the information system; (3) Is	FPT_TUD_EXT.1.1 supports obtaining the TOE version number, which supports the component inventory on the software side.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			at the level of granularity deemed necessary for tracking and reporting; and (4) Includes [*information deemed necessary to achieve effective information system component accountability*]; • Reviews and updates the information system component inventory [*frequency*].	
		SI-2	**Flaw Remediation** Organization… • Identifies, reports, and corrects information system flaws; • Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; • Installs security-relevant software and firmware updates within [*time period*] of the release of the updates; • Incorporates flaw remediation into the organizational configuration management process.	FPT_TUD_EXT.1.2 supports the ability to install updates and correct system flaws.
		SI-7(15)	**Software, Firmware, and Information Integrity** | Code Authentication • Information system implements cryptographic mechanisms to authenticate [*software or firmware components*] prior to installation.	FPT_TUD_EXT.1.3 supports the authentication of components prior to installation.
FPT_STM.1	**Time Stamps** Reliable Time Stamps • Product is able to provide reliable time stamps.	AU-8	**Time Stamps** Information system… • Uses internal system clocks to generate time stamps for audit records • Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*organization-defined granularity of time measurement*].	The SFR talks about providing reliable time stamps, presumably for auditing purposes. Most profiles modify this to integrate with NTP in the environment (giving AU-8(1)), but that is not mandated from the base SFR.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
FTA_SSL_EXT.1	**TOE Access** TSF-initiated Session Locking (Extended) • For local interactive sessions, the product [*selection: locks the session; disables any activity of the user's data access/display devices other than unlocking the session, and requiring that the administrator re-authenticate to the product prior to unlocking the session; terminates the session*] after a Security Administrator-specified time period of inactivity.	AC-11 *Conditionally*	**Session Lock** Information system… • Prevents further access to the system by initiating a session lock after [*time period*] of inactivity or upon receiving a request from a user • Retains the session lock until the user reestablishes access using established identification and authentication procedures.	FTA_SSL_EXT.1.1 supports the product-initiated session lock of AC-11, depending on the assignment value.
		AC-12 *Conditionally*	**Session Termination** • Information system automatically terminates a user session after [*conditions or trigger events requiring session disconnect*].	If the assignment is completed to terminate the session, AC-12 is supported.
FTA_SSL.3	**Session Locking and Termination** TSF-Initiated Termination • Product terminates **a remote interactive session** after a *Security Administrator-configurable time interval of session inactivity*.	AC-12	**Session Termination** • Information system automatically terminates a user session after [*conditions or trigger events requiring session disconnect*].	Complete the assignment in AC-12 to correspond to the time period of user inactivity.
		SC-10	**Network Disconnect** Information system terminates the network connection associated with a communications session at the end of the session or after [*time period*] of inactivity.	SC-10 addresses FTA_SSL.3 for other types of sessions – particularly network sessions (such as web sessions).
FTA_SSL.4	**Session Locking and Termination** User-Initiated Termination • Product allows **Administrator**-initiated termination of the **Administrator**'s own interactive session.	AC-12(1)	**Session Termination** | User-Initiated Logouts / Message Displays Information system… • Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [*information resources*] • Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.	FTA_SSL.4 supports compliance with AC-12(1), at the product level.
FTA_TAB.1	**TOE Access Banners** Default TOE Access Banners • Before establishing **an administrative user** session the product displays a **Security Administrator-specified** advisory notice and consent warning message regarding use of the product.	AC-8	**System Use Notification** Information system… • Displays to users [*system use notification message or banner*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws … and states that: (1) users	FTA_TAB.1 supports satisfaction of AC-8, but only for this product.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			are accessing a U.S. Government information system; (2) usage may be monitored, recorded, and subject to audit; (3) unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and (4) use of the information system indicates consent to monitoring and recording; • Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system • For publicly accessible systems: (1) displays system use information [*conditions*], before granting further access; (2) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (3) includes a description of the authorized uses of the system.	
FTP_ITC.1	**Inter-TSF Trusted Channel** Inter-TSF Trusted Channel • Product **is capable of using [*selection: IPsec, SSH, TLS, HTTPS*] to** provides a communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [*selection: authentication server, [other capabilities]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. • Product permits the product, or the authorized IT entities to initiate communication via the trusted channel. • Product initiates communication via the trusted channel for [*list of services for which the TSF is able to initiate communications*].	AC-17(2)	**Remote Access** | Protection of Confidentiality / Integrity Using Encryption • Information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Depending on the nature of the endpoints, FTP_ITC.1 supports provision of a trusted channel for remote access. The assignment in FTP_ITC.1.3 must indicate the channel is used for remote access.
		IA-3	**Device Identification and Authentication** Information system uniquely identifies and authenticates [*specific and/or types of devices*] before establishing a [*(one or more): local; remote; network*] connection.	FTP_ITC.1 discusses provision of a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. As such, is supports identification of the end-points.
		IA-3(1)	**Device Identification and Authentication** | Cryptographic Bidirectional	FTP_ITC.1 discusses provision of a communication channel

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			Authentication Information system authenticates [*specific devices and/or types of devices*] before establishing [*local; remote; network*] connection using bidirectional authentication that is cryptographically based.	between itself and another trusted IT product. The protocols called out in this control utilize cryptography, and as such, is supports cryptographic identification of the end-points.
		IA-5(1)	**Authenticator Management** | Password-Based Authentication ‡ Information system, for password-based authentication… • […] • Stores and transmits only encrypted representations of passwords […]	FTP_ITC.1 requires protection of channel data from disclosure. If it is refined to use encryption, it would serve to ensure that passwords are transmitted encrypted, supporting IA-5(1) item c.
		SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	FTP_ITC.1 calls for protection of channel data "from modification or disclosure", supporting SC-8.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	FTP_ITC.1 calls for protection of channel data "from modification or disclosure", and cryptographic protocols are called out, thus supporting SC-8(1).
		SC-23	**Session Authenticity** Information system protects the authenticity of communications sessions.	The normal use of trusted channels provides identification of the endpoints, supporting session authenticity.
		Note: SC-11 does not apply, as that calls for a trusted path between the product and **users**. SC-13 does not apply because only the protocols are specified, not the algorithms.		
FTP_TRP.1	**Trusted Path** Trusted Path • Product **can use [*selection: IPsec, SSH, TLS, HTTPS*] to** provide a communication path between itself and **authorized remote administrators** that is logically distinct from other communication paths and	AC-17(2)	**Remote Access** | Protection of Confidentiality / Integrity Using Encryption • Information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	FTP_TRP.1 explicitly uses cryptographic protocols to remote administrators, supporting AC-17(2).

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
	provides assured identification of its end points and protection of the communicated data from *disclosure and provides detection of modification of the channel data*. • Product permits **remote administrators** to initiate communication via the trusted path. • Product requires the use of the trusted path for **initial administrator authentication and all remote administration actions**.	IA-3	**Device Identification and Authentication** Information system uniquely identifies and authenticates [*specific and/or types of devices*] before establishing a [*(one or more): local; remote; network*] connection.	FTP_TRP.1 discusses provision of a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. As such, is supports identification of the end-points.
		IA-3(1)	**Device Identification and Authentication** | Cryptographic Bidirectional Authentication Information system authenticates [*specific devices and/or types of devices*] before establishing [*local; remote; network*] connection using bidirectional authentication that is cryptographically based.	FTP_TRP.1 discusses provision of a communication channel between itself and another trusted IT product. The protocols called out in this control utilize cryptography, and as such, is supports cryptographic identification of the end-points.
		IA-5(1)	**Authenticator Management** | Password-Based Authentication ‡ Information system, for password-based authentication… • […] • Stores and transmits only encrypted representations of passwords • […]	FTP_TRP.1 requires protection of communicated data. If it is completed to protect from disclosure and refined to use encryption, it would serve to ensure that passwords are transmitted encrypted, addressing IA-5(1) item c.
		SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	FTP_TRP.1 calls for protection of channel data “from modification or disclosure”, supporting SC-8.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	FTP_TRP.1 calls for protection of channel data “from modification or disclosure”, and cryptographic protocols are called out, thus supporting SC-8(1).

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
		SC-11	**Trusted Path** Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	FTP_TRP.1 supports establishment of the trusted path.
		SC-23	**Session Authenticity** Information system protects the authenticity of communications sessions.	The normal use of trusted path provides identification of the endpoints, supporting session authenticity.
		Note: Support for SC-11(1) is unclear, due to an unclear distinction between "logically distinct" and "logically isolated", and the fact that the control does not explicitly require that the path be distinguishable from other paths (for HTTPS and TLS you might get that from a browser lock icon, but for other protocols it is unclear).		

6. Security Assurance Requirements

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
ASE_*xxx*	**Security Target Evaluation**	CM-7	**Least Functionality** Organization… • Configures the information system to provide only essential capabilities • Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*prohibited or restricted functions, ports, protocols, and/or services*].	STs and PPs do define security objectives for the operational environment that dictate the restrictions on the operational environment, and often detail what must be prohibited or restricted. This is all part of the evaluated configuration for the product, and is assumed to be followed. This goes to item b. of the control about prohibiting or restricting functions.
		PL-2	**System Security Plan ‡** Organization… 1. Develops a security plan for the information system that: 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the	The information required in the security target in this section supports the overall system security plan, aiding in writing the rationale of how the use of product helps meet controls.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. [⋮] 8. Provides an overview of the security requirements for the system; 9. [⋮] 10. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; 11. [⋮] 12. [⋮]	
		SA-4	**Acquisition Process** Organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service […]: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.	The information in the ST supports the information called out by SA-4
		SA-4(7)	**Acquisition Process** | NIAP-Approved Protection	The conformance claims support SA-4(7) by identifying any

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			Profiles Organization… • Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; • Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.	protection profile claims.
ADV_FSP.1	**Functional Specification** Security-Enforcing Functional Specification • Developer provides a functional specification and a tracing from the functional specification to the SFRs. • Functional specification: 1. Describe the purpose and method of use for each SFR-enforcing and SFR-supporting interface. 2. Identifies all parameters associated with each SFR-enforcing and SFR-supporting interface. 3. Provides rationale for the implicit categorisation of interfaces as SFR-non-interfering. • Tracing demonstrates that the SFRs trace to interfaces in the functional specification. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. • Evaluator determines that the functional specification is an accurate and complete instantiation of the SFRs.	SA-4(1)	**Acquisition Process** | Functional Properties of Security Controls • Organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	The ADV_FSP family provides information about functional interfaces. The SA-4(1) control requires describing the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.
		SA-4(2)	**Acquisition Process** | Design / Implementation Information for Security Controls • Organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*(one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [design/implementation information]*] at [*level of detail*].	The ADV_FSP family provides information about functional interfaces. The SA-4(2) control requires design and implementation information; it should be completed to require them at the level of the security-relevant external system interfaces. **Note**: There is no requirement that requires separation of interfaces into security-enforcing, security non-enforcing, security non-interfering, etc.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
AGD_OPE.1	**Operational User Guidance** Operational User Guidance • Developer provides operational user guidance. • Operational user guidance: 1. Describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. 2. Describes, for each user role, how to use the available interfaces provided by the product in a secure manner. 3. Describes, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate. 4. For each user role, clearly presents each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the product. 5. Identifies all possible modes of operation of the product (including operation following failure or operational error), their consequences and implications for maintaining secure operation. 6. For each user role, describes the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST. 7. Is written to be clear and reasonable. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.	SA-5	**Information System Documentation** Organization… • Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; • Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions / mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; 3. User responsibilities in maintaining the security of the system, component, or service; • [⋮]	AGD_OPE is the combined requirement for administrator and user documentation.
		Note: NIST SP 800-53 parallels the CC v2 approach, which distinguished administrator and user documentation (AGD_USR, AGD_ADM). CC v3 combined these into a single SAR, reflecting the situation that some products do not have non-administrative users.		
AGD_PRE.1	**Preparative Procedures** Preparative Procedures • Developer provides the product including its preparative procedures. • Preparative procedures: 1. Describe all the steps necessary for secure acceptance of the delivered product in accordance with the developer's delivery procedures.	SA-5	**Information System Documentation ‡** Organization… • Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system,	AGD_PRE.1 calls for describing all the steps necessary for secure acceptance and secure delivery. The control calls for documentation or secure configuration and installation.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
	2. Describe all the steps necessary for secure installation of the product and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. • Evaluator applies the preparative procedures to confirm that the product can be prepared securely for operation.		component, or service; 2. […] • […]	
ALC_CMC.1	**CM Capabilities** Labeling of the TOE • Developer provides the product and a reference for the product. • The product is labelled with its unique reference. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.	CM-9	**Configuration Management Plan ‡** Organization develops, documents, and implements a configuration management plan for the information system that… • […] • Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; • […]	At the product level, identification of the configuration items would include identification of the product with a unique reference.
ALC_CMS.1	**CM Scope** TOE CM Coverage • Developer provides a configuration list for the TOE. • Configuration list includes the following: the TOE itself; and the evaluation evidence required by the SARs. • Configuration list uniquely identifies the configuration items. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.	CM-3(6)*	**Configuration Change Control** | Cryptography Management • Organization ensures that cryptographic mechanisms used to provide [*security safeguards*] are under configuration management.	At the product level, if the cryptographic mechanisms providing the safeguards are part of the TOE, they would be covered by CM.
		CM-9	**Configuration Management Plan ‡** Organization develops, documents, and implements a configuration management plan for the information system that… • […] • Defines the configuration items for the information system and places the configuration items under configuration management;. […]	This addresses defining the configuration items and the CM system. Note that ALC_CMC focuses on the *product*, whereas CM-9 focuses on the *system.*
		SA-10	**Developer Configuration Management ‡** Organization requires the developer of the information system, system component, or information system service to:	ALC_CMS captures the "[*configuration items under configuration management*]"

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			• […] • Document, manage, and control the integrity of changes to [*configuration items under configuration management*]; [:]	
ATE_IND.1	**Independent Testing** Independent Testing – Conformance • Developer provides the product for testing. • The product shall be suitable for testing. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. • Evaluator tests a subset of the TSF to confirm that the TSF operates as specified.	CA-2	**Security Assessments** Organization… • Develops a security assessment plan that describes the scope of the assessment including: (1) Security controls and control enhancements under assessment; (2) Assessment procedures to be used to determine security control effectiveness; and (3) Assessment environment, assessment team, and assessment roles and responsibilities; • Assesses the security controls in the information system and its environment of operation [*frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; • Produces a security assessment report that documents the results of the assessment • Provides the results of the security control assessment to [*individuals or roles*].	Independent testing *at the product level* supports testing of the overall system. As such, the *product-level* test plan can support the system-level test plans in terms of eliminating test redundancy, and the results of testing can feed into the system results.
		CA-2(1)	**Security Assessments** | Independent Assessors Organization employs assessors or assessment teams with [*level of independence*] to conduct security control assessments.	Assessment teams for ATE_IND are drawn from NIAP-approved CCTLs that are independent from the developer. However, the CCTLs may not meet the *level of independence* dictated by the SCA.
		Note: ATE_IND.1 only has independent oversight for a portion of the test suite. **Note:** cPPs contain technology-specific assurance activities for each SFR to ensure sufficient testing and sufficiency. When using product evaluations to support assessment and authorization, SCAs should review the assurance activities to determine the extent that they support required control testing. **Note:** Common criteria tests a product in the limited environment defined by the assumptions in the ST. System level testing must test the product in the actual operational environment, and must ensure that all		

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
		assumptions still hold.		
AVA_VAN.1	**Vulnerability Analysis** Vulnerability Survey • Developer provides the product for testing. • The product is suitable for testing. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. • Evaluator performs a search of public domain sources to identify potential vulnerabilities in the product. • Evaluator conducts penetration testing, based on the identified potential vulnerabilities, to determine that the product is resistant to attacks performed by an attacker possessing Basic attack potential.	CA-2(2)	**Security Assessments** | Specialized Assessments • Organization includes as part of security control assessments, [*frequency*], [*announced; unannounced*], [*(one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [other forms of security assessment]*].	If the assignment in CA-2(2) is completed to include a public domain search and subsequent testing of any potential vulnerabilities identified, then AVA_VAN.1 addresses CA-2(2) *at the product level*. **Note:** Vulnerability testing at the product level does not ensure the product integrated into the complete system is configured correctly, nor does it ensure there are no other integration flaws.
		CA-8	**Penetration Testing** Organization conducts penetration testing [*frequency*] on [*information systems or system components*].	**Note:** Although the AVA_VAN.1 controls calls out penetration testing, it is unclear whether it is *required* under the cPP, as Section 6.6 on AVA does not mention penetration testing. If it is performed, it would be only to confirm the presence or absence of the flaws identified through the public domain search.
		SA-11(2)	**Developer Security Testing and Evaluation** | Threat and Vulnerability Analyses Organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.	AVA_VAN requires that there be a vulnerability analysis performed.
		Note: RA-3 and SA-11(5) do not apply. RA-3 is risk assessment, including the likelihood and magnitude of harm, from attacks. It is not the determination of vulnerabilities. Risk assessment can only be done in the context of a particular mission and installation. As for SA-11(5), under the Common Criteria, it is the *evaluator*, not the *developer*, who performs vulnerability assessment.		

A. Optional Requirements

ND cPP Component		NIST SP 800-53 Revision 4 Control	Comments and Observations
A.1	**Audit Events for Optional SFRs**	**Note:** These additional events would correspond to additional values in the assignments for AU-2 and AU-12 (and possibly AU-3(1)), controls	

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
		already addressed in the mandatory requirements. Again, note that the additional events are insufficient to cover all the events called out in CNSSI № 1253.		
FAU_STG.1	**Security Audit Event Storage** Protected Audit Trail Storage • Product protects stored audit records from unauthorized deletion. • Product can prevent unauthorized modifications to stored audit records.	AU-9	**Protection of Audit Information** • Information system protects audit information and audit tools from unauthorized access, modification, and deletion	AU-9 requires that audit information is protected "from unauthorized access, modification, and deletion ". Note that to correspond to AU-9, complete the selection in FAU_STG.1.2 as "prevent". However, the AU-9 control goes beyond the SFR to protect not only the audit trail, but also audit tools.
FAU_STG_EXT.2	**Security Audit Event Storage** Counting lost audit data • Product provides provide information about the number of [*selection: dropped, overwritten, assignment: other information*] audit records in the case where the local storage has been filled and the TSF takes one of the actions defined in FAU_STG_EXT.1.3.	**Note:** This does not appear to correspond or support anything in the 800-53 control set.		
FAU_STG_EXT.3	**Security Audit Event Storage** Display warning for local storage space • Product generates a warning to inform the user before the local • space to store audit data is used up and/or the TOE will lose audit data due to insufficient local space.	AU-5(1)	**Response to Audit Processing Failures** | Audit Storage Capacity • Information system provides a warning to [*personnel, roles, and/or locations*] within [*time period*] when allocated audit record storage volume reaches [*percentage*] of repository maximum audit record storage capacity.	This SFR supports the warnings called out by AU-5(1).
FMT_MOF.1(1)/ Audit	**Management of Functions in TSF** Management of Security Functions Behavior • Product restricts the ability to determine the behaviour of, modify the behaviour of the functions *transmission of audit data to an external IT entity* to *Security Administrators*.	AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Restriction of management functions to particular roles is at least a partial implementation of RBAC.
		AC-6	**Least Privilege** • Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Provision of limited management functionality divided by role supports satisfaction of least privilege. **Note:** Support for the principle of least privilege at a product level does not guarantee it is implemented effectively across the entire system.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
		AU-9(4)	**Protection of Audit Information** | Access by Subset of Privileged Users • Organization authorizes access to management of audit functionality to only [*privileged users*].	This SFR supports the specific restrictions of audit functionality.
FMT_MOF.1(2)/ Audit	**Management of Functions in TSF** Management of Security Functions Behavior • Product restricts the ability to determine the behaviour of, modify the behaviour of the functions *handling of audit data* to *Security Administrators*.	AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Restriction of management functions to particular roles is at least a partial implementation of RBAC.
		AC-6	**Least Privilege** Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Provision of limited management functionality divided by role supports satisfaction of least privilege. **Note:** Support for the principle of least privilege at a product level does not guarantee it is implemented effectively across the entire system.
		AU-9(4)	**Protection of Audit Information** | Access by Subset of Privileged Users Organization authorizes access to management of audit functionality to only [*privileged users*].	This SFR supports the specific restrictions of audit functionality.
FMT_MOF.1(1)/ AdminAct	**Management of Functions in TSF** Management of Security Functions Behavior • Product restricts the ability to modify the behaviour of the functions *TOE Security Functions* to *Security Administrators*.	AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Restriction of management functions to particular roles is at least a partial implementation of RBAC.
		AC-6	**Least Privilege** Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Provision of limited management functionality divided by role supports satisfaction of least privilege. **Note:** Support for the principle of least privilege at a product level does not guarantee it is implemented effectively across the entire system.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
		AU-9(4) *Conditionally*	**Protection of Audit Information** | Access by Subset of Privileged Users Organization authorizes access to management of audit functionality to only [*privileged users*].	If the TOE Security Functions includes audit functionality, then this SFR supports the specific restrictions of audit functionality.
FMT_MOF.1(2)/ AdminAct	**Management of Functions in TSF** Management of Security Functions Behavior • Product restricts the ability to enable, disable of functions *services* to *Security Administrators*.	AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Restriction of management functions to particular roles is at least a partial implementation of RBAC.
		AC-6	**Least Privilege** Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Provision of limited management functionality divided by role supports satisfaction of least privilege. **Note:** Support for the principle of least privilege at a product level does not guarantee it is implemented effectively across the entire system.
FMT_MOF.1/ LocSpace	**Management of Functions in TSF** Management of Security Functions Behavior • Product restricts the ability to determine the behaviour of, modify the behaviour of the functions *audit functionality when Local Audit Storage Space is full* to *Security Administrators*.	AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Restriction of management functions to particular roles is at least a partial implementation of RBAC.
		AC-6	**Least Privilege** Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Provision of limited management functionality divided by role supports satisfaction of least privilege. **Note:** Support for the principle of least privilege at a product level does not guarantee it is implemented effectively across the entire system.
		AU-9(4)	**Protection of Audit Information** | Access by Subset of Privileged Users Organization authorizes access to management of audit functionality to only [*privileged users*].	This SFR supports the specific restrictions of audit functionality.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
FMT_MTD.1/ AdminAct	**Management of TSF Data** Management of TSF Data • Product restricts the ability to modify, delete, generate/import the *cryptographic keys* to *Security Administrators*.	AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Restriction of management functions to particular roles is at least a partial implementation of RBAC.
		AC-6	**Least Privilege** Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Provision of limited management functionality divided by role supports satisfaction of least privilege. **Note:** Support for the principle of least privilege at a product level does not guarantee it is implemented effectively across the entire system.
		IA-7 *Conditionally*	**Cryptographic Module Authentication** • Information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, […] for such authentication.	If the mechanism used to restrict generation / import of cryptographic keys includes authentication to a cryptographic module, this control is supported.
		SC-12	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	This SFR supports, in a broad sense, the management of cryptographic keys.
FPT_FLS.1/ LocSpace	**Fail Secure** Failure with Preservation of Secure State • Product preserves a secure state when the following types of failures occur: [*Local Storage Space for audit data is full*].	AU-9	**Protection of Audit Information** • Information system protects audit information and audit tools from unauthorized access, modification, and deletion	Failing such that audit is preserved supports AU-9
		SC-24	**Fail in Known State** Information system fails to a [*known-state*] for [*types of failures*] preserving [*system state information*] in failure.	Under the presumption that SC-24 is completed to address local audit storage, it is supported by this SFR.

B. Selection-Based Requirements

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
B.1	**Audit Events for Selection-Based SFRs**	**Note:** These additional events would correspond to additional values in the assignments for AU-2 and AU-12 (and possibly AU-3(1)), controls already addressed in the mandatory requirements. Again, note that the additional events are insufficient to cover all the events called out in CNSSI № 1253.		
FCS_HTTPS_EXT.1	**Cryptographic Protocols** HTTPS Protocol • Product implements HTTPS using TLS. • Product does [*selection: not establish the connection, request authorization to establish the connection, no other action*] if the peer certificate is deemed invalid.	SC-5	**Denial of Service Protection** • Information system protects against or limits the effects of the following types of denial of service attacks: [*types of denial of service attacks or reference to source for such information*] by employing [*security safeguards*].	To the extent that the configuration settings for the protocol are present to combat known Denial of Service attacks, this control is supported.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*(one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	HTTPS is a cryptographic mechanism that supports transmission protection.
		SC-11	**Trusted Path** • Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	HTTPS supports establishment of a trusted communication path.
FCS_IPSEC_EXT.1	**Cryptographic Protocols** IPsec Protocol • Product implements the IPsec architecture as specified in RFC 4301. • Product implements [a bunch of specific IPSec sub-protocols, requirements, and settings]	SC-5	**Denial of Service Protection** • Information system protects against or limits the effects of the following types of denial of service attacks: [*types of denial of service attacks or reference to source for such information*] by employing [*security safeguards*].	To the extent that the configuration settings for the protocol are present to combat known Denial of Service attacks, this control is supported.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system	IPSec is a cryptographic mechanism that supports transmission protection.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			implements cryptographic mechanisms to [*(one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	
		SC-11	**Trusted Path** • Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	IPSec supports establishment of a trusted communication path.
		SC-13	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	As the specific configuration requirements dictate specific encryption algorithms, SC-13 is supported.
FCS_SSHC_EXT.1	**Cryptographic Protocols** SSH Client Protocol • Product implements the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and [*selection: 5647, 5656, 6187, 6668, no other RFCs*]. • Product implements [a bunch of specific SSH Client sub-protocols, requirements, and settings]	AC-17(2)	**Remote Access** | Protection of Confidentiality / Integrity Using Encryption • Information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	As SSH is used for remote access, the encryption used support AC-17(2)
		IA-2	**Identification and Authentication (Organizational Users)** • Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	As the SFR requires support for password or PKI based authentication, IA-2 is supported. **Note:** Depending on the type of authentication supported, additional controls and enhancements from the IA-5 family may be addressed – in particular IA-5, IA-5(1), IA-5(2)
		SC-5	**Denial of Service Protection** • Information system protects against or limits the effects of the following types of denial of service attacks: [*types of denial of service attacks or reference to source for such information*] by employing [*security safeguards*].	To the extent that the configuration settings for the protocol are present to combat known Denial of Service attacks, this control is supported.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*(one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	SSH is a cryptographic mechanism that supports transmission protection.
		SC-11	**Trusted Path** • Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	SSH supports establishment of a trusted communication path.
		SC-13	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	As the specific configuration requirements dictate specific encryption algorithms, SC-13 is supported.
FCS_SSHS_EXT.1	**Cryptographic Protocols** SSH Server Protocol • Product implements the SSH protocol that complies with RFCs • 4251, 4252, 4253, 4254, and [*selection: 5647, 5656, 6187, 6668, no other RFCs*]. • Product implements [a bunch of specific SSH Server sub-protocols, requirements, and settings]	AC-17(2)	**Remote Access** | Protection of Confidentiality / Integrity Using Encryption • Information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	As SSH is used for remote access, the encryption used support AC-17(2)
		IA-2	**Identification and Authentication (Organizational Users)** Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	As the SFR requires support for password or PKI based authentication, IA-2 is supported. **Note:** Depending on the type of authentication supported, additional controls and enhancements from the IA-5 family may be addressed – in particular IA-5, IA-5(1), IA-5(2)
		SC-5	**Denial of Service Protection** Information system protects against or limits the effects of the following	To the extent that the configuration settings for the protocol are present to combat known Denial of Service attacks, this

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			types of denial of service attacks: [*types of denial of service attacks or reference to source for such information*] by employing [*security safeguards*].	control is supported.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*(one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	SSH is a cryptographic mechanism that supports transmission protection.
		SC-11	**Trusted Path** Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	SSH supports establishment of a trusted communication path.
		SC-13	**Cryptographic Protection** Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	As the specific configuration requirements dictate specific encryption algorithms, SC-13 is supported.
FCS_TLSC_EXT.1	**Cryptographic Protocols** TLS Client Protocol (without client authentication) • Product implements [*selection: TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] supporting the following ciphersuites [*list*]: • Product implements [a bunch of specific TLS Client sub-protocols, requirements, and settings]	IA-9 *Conditionally*	**Service Identification and Authentication** • Organization identifies and authenticates [*information system services*] using [*security safeguards*].	FCS_TLSC_EXT.1.2 discusses verification that the presented identifier matches the reference identifier according to RFC 6125. The explanation makes it appear that this could support service authentication.
		SC-5	**Denial of Service Protection** • Information system protects against or limits the effects of the following types of denial of service attacks: [*types of denial of service attacks or reference to source for such information*] by employing [*security safeguards*].	To the extent that the configuration settings for the protocol are present to combat known Denial of Service attacks, this control is supported.

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*(one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	TLS is a cryptographic mechanism that supports transmission protection.
		SC-11	**Trusted Path** Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	TLS supports establishment of a trusted communication path.
		SC-13	**Cryptographic Protection** Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	As the specific configuration requirements dictate specific encryption algorithms, SC-13 is supported.
FCS_TLSC_EXT.2	**Cryptographic Protocols** TLS Client Protocol (with client authentication) • Product implements [*selection: TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] supporting the following ciphersuites [*list*]: • Product implements [a bunch of specific TLS Client sub-protocols, requirements, and settings] • Product supports mutual authentication using X.509v3 certificates.	IA-2	**Identification and Authentication (Organizational Users)** Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	The SFR supports endpoint authentication. This is most likely authentication of individuals per X.509 (and they are likely organizational). **Note:** Depending on the usage of the authentication, IA-3 (device authentication), IA-8 (non-organizational users), or IA-9 (service authentication) may also be met. **Note:** The X.509 SFRs address the requirements resulting from certificate validation.
		IA-9 *Conditionally*	**Service Identification and Authentication** • Organization identifies and authenticates [*information system services*] using [*security safeguards*].	FCS_TLSC_EXT.2.2 discusses verification that the presented identifier matches the reference identifier according to RFC 6125. The explanation makes it appear that this could support service

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
				authentication.
		SC-5	**Denial of Service Protection** Information system protects against or limits the effects of the following types of denial of service attacks: [*types of denial of service attacks or reference to source for such information*] by employing [*security safeguards*].	To the extent that the configuration settings for the protocol are present to combat known Denial of Service attacks, this control is supported.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*(one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	TLS is a cryptographic mechanism that supports transmission protection.
		SC-11	**Trusted Path** Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	TLS supports establishment of a trusted communication path.
		SC-13	**Cryptographic Protection** Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	As the specific configuration requirements dictate specific encryption algorithms, SC-13 is supported.
FCS_TLSS_EXT.1	**Cryptographic Protocols** TLS Server Protocol (without client authentication) • Product implements [*selection: TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] supporting the following ciphersuites [*list*]: • Product implements [a bunch of specific TLS Server sub-protocols,	IA-9 *Conditionally*	**Service Identification and Authentication** • Organization identifies and authenticates [*information system services*] using [*security safeguards*].	Although the TLSS_EXT SFR does not discuss verification that the presented identifier matches the reference identifier according to RFC 6125, it is implied by the fact it is communicating with a TLSC_EXT client. The explanation makes it

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
	requirements, and settings]			appear that this could support service authentication.
		SC-5	**Denial of Service Protection** Information system protects against or limits the effects of the following types of denial of service attacks: [*types of denial of service attacks or reference to source for such information*] by employing [*security safeguards*].	To the extent that the configuration settings for the protocol are present to combat known Denial of Service attacks, this control is supported.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*(one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	TLS is a cryptographic mechanism that supports transmission protection.
		SC-11	**Trusted Path** Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	TLS supports establishment of a trusted communication path.
		SC-13	**Cryptographic Protection** Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	As the specific configuration requirements dictate specific encryption algorithms, SC-13 is supported.
FCS_TLSS_EXT.2	**Cryptographic Protocols** TLS Client Protocol (with client authentication) • Product implements [*selection: TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] supporting the following ciphersuites [*list*]: • Product implements [a bunch of specific TLS Server sub-protocols, requirements, and settings] • Product supports mutual	IA-2	**Identification and Authentication (Organizational Users)** Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	The SFR supports endpoint authentication. This is most likely authentication of individuals per X.509 (and they are likely organizational). **Note:** Depending on the usage of the authentication, IA-3 (device authentication), IA-8 (non-organizational users), or IA-9 (service

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
	authentication using X.509v3 certificates.			authentication) may also be met. **Note:** The X.509 SFRs address the requirements resulting from certificate validation.
		IA-9 *Conditionally*	**Service Identification and Authentication** Organization identifies and authenticates [*information system services*] using [*security safeguards*].	Although the TLSS_EXT SFR does not discuss verification that the presented identifier matches the reference identifier according to RFC 6125, it is implied by the fact it is communicating with a TLSC_EXT client. The explanation makes it appear that this could support service authentication.
		SC-5	**Denial of Service Protection** Information system protects against or limits the effects of the following types of denial of service attacks: [*types of denial of service attacks or reference to source for such information*] by employing [*security safeguards*].	To the extent that the configuration settings for the protocol are present to combat known Denial of Service attacks, this control is supported.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*(one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	TLS is a cryptographic mechanism that supports transmission protection.
		SC-11	**Trusted Path** Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	TLS supports establishment of a trusted communication path.
		SC-13	**Cryptographic Protection** Information system implements [*cryptographic*	As the specific configuration requirements dictate specific encryption

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			uses and type of cryptography required for each use] in accordance with applicable federal laws … and standards.	algorithms, SC-13 is supported.
FPT_TST_EXT.2	**TSF Self Test** Self tests based on certificates • Product will fail self-testing if a certificate is used for self tests and the corresponding certificate is deemed invalid.	SI-6	**Security Function Verification** Information system… • Verifies the correct operation of [*security functions*]; • Performs this verification [*(one or more): [system transitional states]; upon command by user with appropriate privilege; [frequency]*]; • Notifies [*personnel or roles*] of failed security verification tests; • [*(one or more): shuts the information system down; restarts the information system; [alternative action(s)]*] when anomalies are discovered.	This testing can support the SI-6 testing.
FPT_TUD_EXT.2	**Trusted Update** Trusted Update based on certificates • Product does not install an update if the code signing certificate is deemed invalid. • When the certificate is deemed invalid because the certificate has expired, product [*selection: allows the administrator to choose whether to accept the certificate in these cases, accepts the certificate, does not accept the certificate*].	CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	FPT_TUD_EXT.2 supports CM-5(3)
FMT_MOF.1(2)/ TrustedUpdate	**Management of Functions in TSF** Management of Security Functions Behavior / Trusted Update • Product restricts the ability to enable, disable the functions *[selection: automatic checking for updates, automatic update]* to [*security administrators*].	AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Restriction of management functions to particular roles supports implementation of RBAC.
		AC-6	**Least Privilege** Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions	Provision of limited management functionality divided by role supports satisfaction of least privilege. **Note:** Support for the principle of least privilege at a product level does not guarantee it is implemented effectively across the

ND cPP Component		NIST SP 800-53 Revision 4 Control		Comments and Observations
			and business functions.	entire system.
		CM-5	**Access Restrictions for Change** • Organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	This SFR supports the ability to restrict who can configure changes (updates).
		SI-2(5)	**Flaw Remediation** | Automatic Software / Firmware Updates • Organization installs [*software and firmware updates*] automatically to [*information system components*].	Permitting automatic updates supports SI-2(5).