Mapping Between

Collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020

and

NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253 are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context**. Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to generate audit records only supports AU-2 to the extent that the TOE's audit records are included in the set of "organization-defined auditable events" assigned by that control. The security control assessor must compare the TOE's functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
Mandatory Requirements				
FAU_GEN.1	<u>**Audit Data Generation**</u>	AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-12	**Audit Record Generation**	A conformant TOE has the ability to generate audit logs. The TOE supports the enforcement of parts (a) and (c) of the control if its auditable events are consistent with the assignments chosen for the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				control and if the TOE's audit log is part of the overall system's auditing. Part (b) is not satisfied by a conformant TOE because the PP does not define functionality to suppress/enable the generation of specific audit records (which would typically be expressed in CC as FAU_SEL.1).
FAU_GEN.2	**User Identity Association**	AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
FAU_STG_EXT.1	**Protected Audit Event Storage**	AU-4	**Audit Log Storage Capacity**	A conformant TOE allocates some amount of local storage for audit data. It can be used to support the enforcement of this control if the amount of storage is consistent with the assignment chosen for the control.
		AU-4(1)	**Audit Log Storage Capacity:** Transfer to Alternate Storage	A conformant TOE has the ability to logically transmit audit data to a location in its Operational Environment. While this SFR requires the TSF to store generated audit data on the TOE, a minimum storage size or retention period is not specified. Therefore, a TOE may support the enforcement of this control if the local

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				storage of audit data is limited or transitory.
		AU-5	**Response to Audit Logging Process Failures**	A conformant TOE has the ability to react in a specific manner when the allocated audit storage space is full. Depending on the actions taken by the TOE when this occurs and on the assignments chosen for this control, the TOE can be used to support the enforcement of either or both parts of the control.
		AU-5(2)	**Response to Audit Logging Process Failures:** Real-Time Alerts	A conformant TOE has the ability to react in a specific manner when the allocated audit storage space is full. A conformant TOE may support the enforcement of this control, depending on the behavior specified in the ST and the assignments chosen for this control.
		AU-5(4)	**Response to Audit Logging Process Failures:** Shutdown on Failure	A conformant TOE has the ability to react in a specific manner when the allocated audit storage space is full. A conformant TOE may support the enforcement of this control, depending on the behavior specified in the ST and the assignments chosen for this control.
		AU-9	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records.
		AU-9(2)	**Protection of Audit Information:** Store on Separate Physical Systems or Components	A conformant TOE must be able to transmit audit data to a logically remote location. It can be used to support the enforcement of this control if the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				recipient of the audit data is physically remote from the TOE.
FCS_CKM.1	**Cryptographic Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate asymmetric keys satisfies the key generation portion of this control.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE ensures that generated asymmetric keys provide an appropriate level of security.
FCS_CKM.2	**Cryptographic Key Establishment**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports this control by providing a key establishment function.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE supports the production of asymmetric keys by providing a key establishment function.
FCS_CKM.4	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_COP.1/ DataEncryption	**Cryptographic Operation (AES Data Encryption/ Decryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/SigGen	**Cryptographic Operation (Signature Generation and Verification)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/Hash	**Cryptographic Operation (Hash Algorithm)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic hashing using NSA-approved and FIPS-validated algorithms.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FCS_COP.1/ KeyedHash	**Cryptographic Operation (Keyed Hash Algorithm)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform keyed-hash message authentication using NSA-approved and FIPS-validated algorithms.
FCS_RBG_EXT.1	**Random Bit Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of an appropriate DRBG ensures that generated keys provide an appropriate level of security.
FIA_AFL.1	**Authentication Failure Management**	AC-7	**Unsuccessful Logon Attempts**	The TOE has the ability to detect when a defined number of unsuccessful authentication attempts occurs and take some corrective action.
FIA_PMG_EXT.1	**Password Management**	IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE will have the ability to enforce some minimum password complexity requirements, although they are not identical to CNSS or DoD requirements or to those specified in part (a) of this control.
FIA_UIA_EXT.1	**User Identification and Authentication**	AC-8	**System Use Notification**	A conformant TOE will display a warning banner before user authentication.
		AC-14	**Permitted Actions Without Identification or Authentication**	A conformant TOE will define a list of actions that are permitted prior to authentication.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE has the ability to require that certain functions require successful authentication to access.
FIA_UAU_EXT.2	**Password-Based Authentication**	IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE may have the ability to authenticate users with a password-based authentication mechanism.
		IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE may have the ability to authenticate users with a

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				public key-based authentication mechanism.
FIA_UAU.7	**Protected Authentication Feedback**	IA-6	**Authentication Feedback**	The TOE is required to provide obscured feedback to the user while authentication is in progress.
FMT_MOF.1/ ManualUpdate	**Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit application of a TOE update unless proper authorization is provided.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to perform manual updates of the TOE software/firmware.
FMT_MTD.1/ CoreData	**Management of TSF Data**	AC-3	**Access Enforcement**	A conformant TOE will not permit manipulation of its stored data unless proper authorization is provided.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to manage TSF data.
FMT_SMF.1	**Specification of Management Functions**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional capabilities defined in this SFR. In general, a conformant TOE will satisfy this control to the extent that the TOE provides a method to configure its behavior in accordance with organizational

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE.
FMT_SMR.2	**Restrictions on Security Roles**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE has the ability to associate users with roles, in support of part (a) of the control.
FPT_APW_EXT.1	**Protection of Administrator Passwords**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to administrative credentials, which supports the control to the extent that such a repository is identified by the organization as requiring restricted access.
		IA-5	**Authenticator Management**	A conformant TOE protects authentication data from unauthorized disclosure, in support of part (g) of this control.
		IA-5(6)	**Authenticator Management:** Protection of Authenticators	A conformant TOE must have the ability to securely store passwords and any other credential data it uses.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE uses a cryptographic mechanism to prevent credential data at rest from being stored in plaintext.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FPT_SKP_EXT.1	**Protection of TSF Data**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to the key storage repository, which supports this control if such a repository is identified by the organization as requiring restricted access.
		IA-5	**Authenticator Management**	If the stored key data includes an authenticator (such as an SSH private key), a conformant TOE protects authentication data from unauthorized disclosure, in support of part (g) of this control.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by protecting stored cryptographic data. If that cryptographic data includes authentication data, it supports IA-5 part (g) as well.
FPT_TST_EXT.1	**TSF Testing**	SI-6	**Security and Privacy Function Verification**	A conformant TOE will run automatic tests to ensure correct operation of its own functionality.
		SI-7	**Software, Firmware, and Information Integrity**	One of the self-tests the TOE may perform is an integrity test of its own software or firmware.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	One of the self-tests the TOE may perform is an integrity test of its own software or firmware.
FPT_TUD_EXT.1	**Trusted Update**	CM-14	**Signed Components**	A conformant TOE requires that updates to it include integrity measures. Depending on the selection made in the SFR, this may include a digital signature.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to it.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FPT_STM_EXT.1	**Reliable Time Stamps**	AU-8	**Time Stamps**	A conformant TOE can generate or use time stamps to address the actions defined in this control.
		SC-45(1)	**System Time Synchronization:** Synchronization with Authoritative Time Source	A conformant TOE may have the ability to synchronize with an NTP server in its operational environment, satisfying this control.
FTA_SSL_EXT.1	**TSF-Initiated Session Locking**	AC-11	**Device Lock**	A conformant TOE may have the ability to lock an idle local interactive session, depending on the selection made in the SFR.
		AC-12	**Session Termination**	A conformant TOE may have the ability to terminate an idle local interactive session, depending on the selection made in the SFR.
		IA-11	**Re-Authentication**	A conformant TOE may have the ability to require user re-authentication after the termination an idle local interactive session, depending on the selection made in the SFR.
FTA_SSL.3	**TSF-Initiated Termination**	AC-2(5)	**Account Management:** Inactivity Logout	A conformant TOE will have the ability to log out after a period of inactivity.
		AC-12	**Session Termination**	A conformant TOE will have the ability to terminate an idle remote interactive session.
FTA_SSL.4	**User-Initiated Termination**	AC-12(1)	**Session Termination:** User-Initiated Logouts	A conformant TOE has the ability to terminate an active session upon user request.
FTA_TAB.1	**Default TOE Access Banners**	AC-8	**System Use Notification**	A conformant TOE displays an advisory warning to the user prior to authentication.
		AC-14	**Permitted Actions Without Identification or Authentication**	A conformant TOE displays an advisory warning to the user prior to authentication.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		PL-4	**Rules of Behavior**	The TOE displays an advisory warning to the user prior to authentication to identify the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy.
FTP_ITC.1	**Inter-TSF Trusted Channel**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocol(s) used to establish trusted communications uses mutual authentication.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
FTP_TRP.1/Admin	**Trusted Path**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocol(s) used to establish trusted communications uses mutual authentication.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE will have the ability to prevent unauthorized disclosure of information and detect modification to that information.
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself.
Optional Requirements				

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FAU_STG.1	**Protected Audit Trail Storage**	AU-9	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records.
		AU-9(6)	**Protection of Audit Information:** Read-Only Access	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records. If the TOE prevents this by preventing all modification and deletion of audit records (i.e., there is no 'authorized' ability to do this), it can be used to support the enforcement of this control.
FAU_STG_EXT.2/ LocSpace	**Counting Lost Audit Data**	AU-5	**Response to Audit Logging Process Failures**	A conformant TOE has the ability to count the amount of audit data that is lost by audit processing failures. This may be used to support the enforcement of this control if such an action is consistent with the assignment specified in part (b) of the control.
FAU_STG_EXT.3/ LocSpace	**Action in Case of Possible Audit Data Loss**	AU-5	**Response to Audit Logging Process Failures**	A conformant TOE will have the ability to generate a warning if local audit storage space is exhausted. This may be used to support the enforcement of part (a) of this control if the method of issuing the warning qualifies as an 'alert.'
		AU-5(1)	**Response to Audit Logging Process Failures:** Storage Capacity Warning	A conformant TOE will have the ability to generate a warning if local audit storage space is exhausted. This may be used to support the enforcement of this control if the TOE's behavior is consistent with the assignments chosen

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				for this control (e.g., since the SFR applies when audit storage space is fully exhausted the final assignment must be '100%').
FIA_X509_EXT.1/ ITT	**Certificate Validation**	IA-3	**Device Identification and Authentication**	A conformant TOE uses X.509 certificates to perform device authentication of distributed TOE components.
		IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	The TOE uses X.509 certificate authentication between distributed components to establish cryptographically-secured communications between them. Establishment of these channels may require bidirectional (mutual) authentication.
		IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to validate certificate path and status, which satisfies this control.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	The TOE's use of X.509 certificates to authenticate distributed components ensures that it will include the functionality needed to validate certificate authorities.
FPT_ITT.1	**Basic Internal TSF Data Transfer Protection**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing a protected communication channel between remote distributed TOE components.
		SC-8(1)	**Transmission Confidentiality and Integrity**: Cryptographic Protection	A conformant TOE will use cryptographic methods to protect data in transit between different parts of the TOE.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FTP_TRP.1/Join	**Trusted Path**	IA-3	**Device Identification and Authentication**	A conformant TOE supports the enforcement of this control by providing a registration mechanism that allows distributed TOE components to identify and authenticate to each other.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support enforcement of this control by providing a protected communication channel between remote distributed TOE components as a method to transmit registration information.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE will use cryptographic methods to protect initial registration data transmitted between different parts of the TOE.
FCO_CPC_EXT.1	**Component Registration Channel Definition**	AC-4	**Information Flow Enforcement**	A conformant TOE supports the enforcement of this control by providing a registration mechanism that is used as a condition for distributed TOE components to establish information flow between them.
FCS_DTLSC_EXT.2	**DTLS Client Support for Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications and provides its own client certificate to the peer, supporting this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:**	The TOE supports a cryptographic method of protecting data in transit.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			Cryptographic Protection	
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_DTLSS_EXT.2	**DTLS Server Support for Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_TLSC_EXT.2	**TLS Client Support for Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications and provides its own client certificate to the peer, supporting this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_TLSS_EXT.2	**TLS Server Support for Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
Selection-Based Requirements				
FAU_GEN_EXT.1	**Security Audit Generation**	AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events. The TOE supports the enforcement of the control

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				by identifying the specific auditable events that are generated by each individual TOE component.
		AU-3	**Content of Audit Records**	In addition to the audit information that is required by FAU_GEN.1.2, a conformant TOE will uniquely identify the individual TOE component that generates each audit record.
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	In addition to the audit information that is required by FAU_GEN.1.2, a conformant TOE will uniquely identify the individual TOE component that generates each audit record.
		AU-12	**Audit Record Generation**	A conformant TOE supports the enforcement of this control by having each of its distributed components generate audit records. The extent to which the TOE supports the enforcement of this control depends on the specific auditable events that are performed by the TSF as a whole, as stated in the mapping to FAU_GEN.1.
FAU_STG_EXT.4	**Protected Local Audit Event Storage for Distributed TOEs**	AU-4	**Audit Log Storage Capacity**	A conformant TOE allocates in each of its distributed components some amount of local storage for audit data. It can be used to support the enforcement of this control if the amount of storage is consistent with the assignment chosen for the control.
		AU-5	**Response to Audit Logging Process Failures**	A conformant TOE has the ability for each of its distributed components to react in a specific manner when the allocated audit storage space for a

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				component is full. Depending on the actions taken by the TOE when this occurs and on the assignments chosen for this control, the TOE can be used to support the enforcement of either or both parts of the control.
		AU-5(2)	**Response to Audit Logging Process Failures:** Real-Time Alerts	A conformant TOE has the ability to react in a specific manner when the allocated audit storage space for one of its distributed components is full. A conformant TOE may support the enforcement of this control, depending on the behavior specified in the ST and the assignments chosen for this control.
		AU-5(4)	**Response to Audit Logging Process Failures:** Shutdown on Failure	A conformant TOE has the ability to react in a specific manner when the allocated audit storage space for one of its distributed components is full. A conformant TOE may support the enforcement of this control, depending on the behavior specified in the ST and the assignments chosen for this control.
FAU_STG_EXT.5	**Protected Remote Audit Event Storage for Distributed TOEs**	AU-4(1)	**Audit Log Storage Capacity:** Transfer to Alternate Storage	A conformant TOE has the ability to buffer local audit records on its distributed components until this data is transferred to a central component that is used for storing audit records.
		AU-9	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of buffered audit records that reside on distributed components while awaiting transfer to a centralized location.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		AU-9(2)	**Protection of Audit Information:** Store On Separate Physical Systems Or Components	A conformant TOE must be able to transmit audit data from distributed components to a centralized component on another part of the TOE. It can be used to support the enforcement of this control if the recipient of the audit data is physically remote from the distributed component. Also note that the TOE may support the enforcement of this control if centralization of data from distributed components is an intermediate step in satisfying FAU_STG_EXT.1.
		AU-12(1)	**Audit Record Generation:** System-Wide and Time-Correlated Audit Trail	A conformant TOE will consolidate the audit logs from its distributed components at a single point within the TOE. However, this SFR does not specify a minimum level of tolerance for time correlation.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit between its distributed components.
FCS_DTLSC_EXT.1	**DTLS Client Protocol Without Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications, supporting this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_DTLSS_EXT.1	**DTLS Server Protocol Without Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE provides a server certificate to a TLS client before establishing trusted communications, supporting this control
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_HTTPS_EXT.1	**HTTPS Protocol**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE may support the implementation of PKI-based authentication by validating peer certificates as part of the authentication process.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		SC-8 (1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_IPSEC_EXT.1	**IPsec Protocol**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE implements peer authentication for IPsec.
		SC-7(5)	**Boundary Protection:** Deny by Default - Allow by Exception	A conformant TOE's IPsec implementation includes a default-deny posture in its SPD.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements IPsec as a method of ensuring confidentiality and integrity of data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE's use of IPsec provides a cryptographic means to protect data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_NTP_EXT.1	**NTP Protocol**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-45(1)	**System Time Synchronization:** Synchronization with Authoritative Time Source	A conformant TOE supports the enforcement of part (a) of this control by providing a mechanism to obtain time data from an authoritative NTP server. This SFR does not discuss drift correction so it is not applicable to part (b) of this control.
		SC-45(2)	**System Time Synchronization:** Secondary Authoritative Time Source	This SFR provides a mechanism to support the enforcement of this control by requiring the TSF to support multiple separate NTP servers as authoritative time sources. However, the SFR does not enforce the geographical separation of these NTP servers so a conformant TOE does not force the implementation of this control on its own.
FCS_SSHC_EXT.1	**SSH Client Protocol**	AC-17(2)	**Remote Access:** Protection of Confidentiality and Integrity Using Encryption	The SSH client protocol implemented by the TOE provides confidentiality and integrity for remote access.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE may use its SSH client functionality to interact with a remote system on behalf of an organizational user.
		IA-3	**Device Identification and Authentication**	A conformant TOE may use its SSH client functionality to establish a static or as-needed connection to a specific remote device that is authenticated using a public key or X.509 certificate (instead of an administrator-supplied

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				credential), which supports this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE's use of SSH supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_SSHS_EXT.1	**SSH Server Protocol**	AC-17(2)	**Remote Access:** Protection of Confidentiality and Integrity Using Encryption	The SSH client protocol implemented by the TOE provides confidentiality and integrity for remote access.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE provides SSH server functionality that enforces identification and authentication of organizational users attempting to access the TSF.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:**	The TOE's use of SSH enforces a cryptographic method of protecting data in transit.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			Cryptographic Protection	
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_TLSC_EXT.1	**TLS Client Protocol Without Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications, supporting this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_TLSS_EXT.1	**TLS Server Protocol Without Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE provides a server certificate to a TLS client before establishing trusted communications, supporting this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FIA_X509_EXT.1/ Rev	**X.509 Certificate Validation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to validate certificate path and status, which satisfies this control.
		SC-23	**Session Authenticity**	Depending on the TOE's use of trusted communications channels, it may use X.509 certificate validation in support of session authentication.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	If the TOE uses X.509 certificates as part of session authentication, it will include the functionality needed to validate certificate authorities.
FIA_X509_EXT.2	**X.509 Certificate Authentication**	IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE has the ability to identify and authenticate organizational users via X.509 certificates. Other controls apply If the TOE also uses code signing certificates for software updates (CM-14), SI-7(15)) or integrity verification (SI-7, SI-7(1), SI-7(6)).
FIA_X509_EXT.3	**X.509 Certificate Requests**	SC-17	**Public Key Infrastructure Certificates**	This function supports behavior related to certificate issuance.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FPT_TUD_EXT.2	**Trusted Update Based on Certificates**	CM-14	Signed Components	A conformant TOE supports the enforcement of this control by using code signing certificates for software updates.
		SI-7(15)	**Software, Firmware, and Information Integrity:** Code Authentication	A conformant TOE's use of a code signing certificate for software updates supports the enforcement of this control.
FMT_MOF.1/ Services	**Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit starting and stopping of services unless proper authorization is provided.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to start and stop services.
FMT_MOF.1/ AutoUpdate	**Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit enabling of automatic updates unless proper authorization is provided.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to configure automatic updates.
		SI-2(5)	**Flaw Remediation:** Automatic Software and Firmware Updates	A conformant TOE will have the ability to have software or firmware updates be configured to occur automatically.
FMT_MOF.1/ Functions	**Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit management of audit behavior unless proper authorization is provided. Note specifically

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				that the functions that this SFR restricts access to relate to configuration of the audit behavior, which relates to the enforcement of AU-5 and AU-9.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to configure audit behavior.
FMT_MTD.1/ CryptoKeys	**Management of TSF Data**	AC-3	**Access Enforcement**	A conformant TOE will not permit manipulation of cryptographic data unless proper authorization is provided. Note specifically that the functions that this SFR restricts access to relate to configuration of the audit behavior, which relates to the enforcement of AC-3(11).
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to interact with cryptographic data.
Objective Requirements				
This PP has no objective requirements.				