Mapping Between
Collaborative Protection Profile for Stateful Traffic Filter Firewalls,
Version 2.0 + Errata 20180314, 14-March-2018
and
NIST SP 800-53 Revision 4

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.
- **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		**Supports Enforcement of NIST SP 800-53 Revision 4 Control**		**Comments and Observations**
FAU_GEN.1	**Audit Data Generation**	AU-2	**Auditable Events**	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 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 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 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 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 storage of audit data is limited or transitory.

		AU-5	**Response to Audit Processing 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 Processing 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 Processing 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:** Audit Backup on Separate Physical Systems / 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 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.
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**	A conformant TOE's use of an appropriate DRBG ensures that generated

			Establishment and Management	keys provide an appropriate level of security.
FDP_RIP.2	**Full Residual Information Protection**	SC-4	**Information in Shared Resources**	A conformant TOE supports this control by ensuring that memory buffers used to temporarily store network packet data cannot be used to that same data in a different packet.
		SC-8(2)	**Transmission Confidentiality and Integrity:** Pre / Post Transmission Handling	A conformant TOE supports this control by ensuring the confidentiality of network packet data.
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 occur 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-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 will have the ability to authenticate users with a password-based authentication mechanism.
FIA_UAU.7	**Protected Authentication Feedback**	IA-6	**Authenticator 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 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:** Role-Based Schemes	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**	IA-5	**Authenticator Management**	A conformant TOE protects authentication data from unauthorized disclosure, in support of part h) 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.
FPT_SKP_EXT.1	**Protection of TSF Data**	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 (h) as well.
FPT_TST_EXT.1	**TSF Testing**	SI-6	**Security 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.
FPT_TUD_EXT.1	**Trusted Update**	CM-5(3)	**Access Restrictions for Change:** 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 itself.
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.
		AU-8(1)	**Time Stamps:** 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	**Session Locking**	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.
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 / Message Displays	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.
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 or Alternate Physical Protection	The TOE supports a cryptographic method of protecting data in transit.
FTP_TRP.1/Admin	**Trusted Path**	IA-3(1)	**Device Identification and**	A conformant TOE may support the enforcement

			Authentication: Cryptographic Bidirectional Authentication	of this control if the protocol(s) used to establish trusted communications uses mutual authentication.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic For Alternate Physical Protection	A conformant TOE will have the ability to prevent unauthorized disclosure of information and detect modification to that information.
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself.
FFW_RUL_EXT.1	**Stateful Traffic Filtering**	SC-7	**Boundary Protection**	A conformant TOE supports the enforcement of this control by acting as a boundary device for its managed interfaces.
		SC-7(4)	**Boundary Protection:** External Telecommunications Services	A conformant TOE supports the enforcement of parts (a) and (b) of this control by enforcing traffic policy rules on managed interfaces. Part (c) is not enforced by the TOE because is it not responsible for the encryption of through traffic, and parts (d) and (e) are not enforced because these relate to organizational policies.
		SC-7(5)	**Boundary Protection:** Deny by Default / Allow by Exception	A conformant TOE denies network communication traffic by default and allows network communication traffic by exception (i.e., deny all, permit by exception) at the managed interfaces.
		SC-7(11)	**Boundary Protection:** Restrict Incoming Communications Traffic	A conformant TOE determines that the source and destination address pairs represent authorized/allowed communications.
Optional Requirements				
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 Processing 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.3/ LocSpace	**Action in Case of Possible Audit Data Loss**	AU-5	**Response to Audit Processing 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 Processing Failures:** Audit Storage Capacity	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 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:** PKI-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.
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_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.

		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.
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 or Alternate Physical Protection	A conformant TOE will use cryptographic methods to protect data in transit between different parts of the TOE.
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 or Alternate Physical 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.
FFW_RUL_EXT.2	**Stateful Filtering of Dynamic Protocols**	SC-7(17)	**Boundary Protection:** Automated Enforcement of Protocol Formats	A conformant TOE dynamically defines rules or establishes sessions allowing network traffic to flow for supported network protocols.
Selection-Based Requirements				
FCS_DTLSC_EXT.1	**DTLS Client Protocol**	IA-5(2)	**Authenticator Management:** PKI-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 or Alternate Physical 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_DTLSC_EXT.2	**DTLS Client Protocol – with Authentication**	IA-5(2)	**Authenticator Management:** PKI-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:** Cryptographic or Alternate Physical 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_DTLSS_EXT.1	**<u>DTLS Server Protocol</u>**	IA-5(2)	**Authenticator Management:** PKI-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 or Alternate Physical 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_DTLSS_EXT.2		IA-5(2)	**Authenticator Management:**	The TOE requires peers to possess a valid certificate before establishing trusted

	DTLS Server Protocol with Mutual Authentication		PKI-Based Authentication	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 or Alternate Physical 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:** PKI-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.
		SC-8 (1)	**Transmission Confidentiality and Integrity:** Cryptographic or Alternate Physical 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:** PKI-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 or Alternate Physical 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_SSHC_EXT.1	**SSH Client Protocol**	AC-17(2)	**Remote Access:** Protection of Confidentiality / 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 it's 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 it's 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 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 or Alternate Physical 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 / 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 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 or	The TOE's use of SSH enforces a cryptographic method of protecting data in transit.

			Alternate Physical 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**	IA-5(2)	**Authenticator Management:** PKI-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 or Alternate Physical 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 Protocol with Authentication**	IA-5(2)	**Authenticator Management:** PKI-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:** Cryptographic or Alternate Physical 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**	IA-5(2)	**Authenticator Management:** PKI-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 or Alternate Physical 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 Protocol with Mutual Authentication**	IA-5(2)	**Authenticator Management:** PKI-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 or Alternate Physical 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	**Certificate Validation**	IA-5(2)	**Authenticator Management:** PKI-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	**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-5(3), SI-7(15))

				or integrity verification (SI-7, SI-7(1), SI-7(6)).
FIA_X509_EXT.3	**Certificate Requests**	SC-17	**Public Key Infrastructure Certificates**	This function supports behavior related to certificate issuance.
FPT_TST_EXT.2	**Self-Tests Based on Certificates**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE supports the enforcement of this control by using a Code Signing certificate as a method of integrity verification.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE supports the enforcement of this control by using a Code Signing certificate to verify the TOE's software/firmware integrity.
		SI-7(12)	**Software, Firmware, and Information Integrity:** Integrity Verification	A conformant TOE supports the enforcement of this control by providing a mechanism to verify the integrity of installed software updates.
FPT_TUD_EXT.2	**Trusted Updates Based on Certificates**	CM-5(3)	**Access Restrictions for Change:** 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/ 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 / 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.
		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.