Mapping Between

Collaborative Protection Profile for Network Devices,

Version 2.1, 11-March-2019

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 Criter	ia Version 3.x SFR		Enforcement of NIST 3 Revision 4 Control	Comments and Observations
FAU_GEN.1	Audit Data	AU-2	Auditable Events	A conformant TOE has the
	Generation			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	A conformant TOE will
			Records	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	A conformant TOE will
			Records:	ensure that audit records
			Additional Audit	include date, type,
			Information	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
		A11.42	A. dia C.	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

	T		Т	
				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	<u>User Identity</u>	AU-3	Content of Audit	A conformant TOE will
	<u>Association</u>		Records	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
FALL CTC EVT 1	Ductostad Audit	AU-4	Audit Ctorogo	overall system's auditing. A conformant TOE
FAU_STG_EXT.1	Protected Audit	AU-4	Audit Storage	
	Event Storage		Capacity	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	A conformant TOE has the
			Capacity: Transfer	ability to logically transmit
			to Alternate	audit data to a location in
			Storage	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 AU-5 (2) Response to Audit Processing Failures AU-5(2) Response to Audit Processing Failures AU-5(2) Response to Audit Processing Failures: Real- Time Alerts AU-5(4) Response to Audit Processing Failures: Response to Audit Processing Failures: Real- Time Alerts AU-5(4) Response to Audit Processing Failures: Response to Audit Processing Failures: Real- Time Alerts AU-5(4) Response to Audit Processing Failures: Audit Storage Space is full. A conform TOE may support the enforcement of this control, depending on behavior specified in ti ST and the assignment chosen for this control Audit Processing Failures: Shutdown on allocated audit storage manner when the ability to react in a spe manner when the allocated audit storage manner when the ability to react in a spe manner when the allocated audit storage	g on e e nd osen E the or ol.
Failures manner when the allocated audit storage space is full. Depending the actions taken by the TOE when this occurs a on the assignments of for this control, the TO can be used to support enforcement of either both parts of the control Addit Processing Failures: Real-Time Alerts AU-5(2) Response to Audit Processing Failures: Real-Time Alerts Allocated audit storage space is full. A conform TOE may support the enforcement of this control, depending on behavior specified in the ST and the assignment chosen for this control AU-5(4) Response to Audit Processing Failures: Shutdown on manner when the allocated audit storage space is full. A conform TOE may support the enforcement of this control, depending on behavior specified in the ST and the assignment chosen for this control and the assignment specified in the ST and the assignment chosen for this control and the assignment specified in the ST and the assignment chosen for this control and the assignment specified in the ST and the assignment chosen for this control and the support of the ST and the assignment specified in the ST and the additional specified in the ST and the action s	g on e nd osen E the or ol the
allocated audit storage space is full. Depending the actions taken by the TOE when this occurs a on the assignments che for this control, the TO can be used to support enforcement of either both parts of the control. AU-5(2) Response to Audit Processing Failures: Real- Time Alerts AU-5(4) Response to Audit Processing Failures: AU-5(4) Response to Audit Processing Failures: AU-5(4) Response to Audit Processing Failures: Shutdown on AU-5(4) AU	g on e nd osen E the or ol. the
space is full. Depending the actions taken by the TOE when this occurs a on the assignments che for this control, the TO can be used to support enforcement of either both parts of the control Audit Processing Failures: Real-Time Alerts AU-5(2) Response to Audit Processing Failures: Shutdown on AU-5(4)	g on e nd osen E the or ol. the
the actions taken by th TOE when this occurs a on the assignments che for this control, the TO can be used to support enforcement of either both parts of the contr Audit Processing Failures: Real- Time Alerts Audit Processing Failures: Real- Time Alerts Audit Aconform TOE may support the enforcement of this control, depending on behavior specified in th ST and the assignment chosen for this control AU-5(4) Response to Audit Processing Failures: Shutdown on Audicated audit storage ability to react in a spe	e nd osen E the or ol. the
AU-5(2) Response to Audit Processing Failures: Real- Time Alerts AU-5(4) Response to AU-5(4) AU-5(4) Response to AU-5(4) AU-5(4) Response to AU-5(4) AU-5(4) Response to AU-5(4) AU-5(4	nd osen E the or ol. the cific
AU-5(2) Response to Audit Processing Failures: AU-5(4) AU-5(4) Response to Audit Processing Failures: Shutdown on AU-5(4) Response to Audit Processing Failures: Shutdown on On the assignments chrifter for this control, the TO Can be used to support enforcement of either both parts of the control A conformant TOE has ability to react in a speemanner when the allocated audit storage space is full. A conformation TOE may support the enforcement of this control, depending on behavior specified in the ST and the assignment chosen for this control ability to react in a speemanner when the allocated audit storage manner when the allocated audit storage manner when the allocated audit storage ability to react in a speemanner when the allocated audit storage allocate	the or ol.
AU-5(2) Response to Audit Processing Failures: Real- Time Alerts AU-5(4) Response to Audit Processing Failures: Shutdown on AU-5(4) Response to AU-5(4) Response to Audit Processing Failures: Shutdown on AU-5(4) AU-5(4) Response to AU-5(4) Response to Audit Processing Failures: Shutdown on AU-5(4) AU-5(4) AU-5(4) Response to Audit Processing Failures: Shutdown on AU-5(4) AU-5(4)	the or ol. the cific
AU-5(2) Response to Audit Processing Failures: Real- Time Alerts AU-5(4) Response to Audit Processing Failures: Real- Time Alerts AU-5(4) Response to Audit Processing Failures: Real- Time Alerts AU-5(4) Response to Audit Processing Failures: Shutdown on Can be used to support enforcement of either both parts of the control A conformant TOE has ability to react in a spen of this control AU-5(4) Response to Audit Processing Failures: Shutdown on A conformant TOE has ability to react in a spen of the control of the con	the or ol. the cific
AU-5(2) Response to Audit Processing Failures: Real- Time Alerts AU-5(4) Response to Audit Processing Failures: Real- Time Alerts AU-5(4) Response to Audit Processing Failures: AU-5(4) Response to Audit Processing Audit Processing Failures: Audit Processing Failures: Audit Processing Failures: Shutdown on Audit Processing Failures: Audit	or ol. the cific
AU-5(2) Response to Audit Processing Failures: Real- Time Alerts AU-5(4) AU-5(4) Response to A conformant TOE has ability to react in a speemanner when the allocated audit storage space is full. A conform TOE may support the enforcement of this control, depending on behavior specified in the ST and the assignment chosen for this control AU-5(4) Response to A conformant TOE has ability to react in a speemanner when the Shutdown on allocated audit storage	ol. the cific
AU-5(2) Response to Audit Processing Failures: Real- Time Alerts Allocated audit storage space is full. A conform TOE may support the enforcement of this control, depending on behavior specified in the ST and the assignment chosen for this control AU-5(4) Response to Audit Processing Failures: Building A conformant TOE has ability to react in a specified in the specified in	the cific
Audit Processing Failures: Real- Time Alerts Allocated audit storage space is full. A conform TOE may support the enforcement of this control, depending on behavior specified in the ST and the assignment chosen for this control AU-5(4) Response to Audit Processing Failures: Shutdown on Ability to react in a speem ability to react in a speem anner when the allocated audit storage	cific
Failures: Real- Time Alerts Failures: Real- Time Alerts allocated audit storage space is full. A conform TOE may support the enforcement of this control, depending on behavior specified in the ST and the assignment chosen for this control AU-5(4) Response to A conformant TOE has ability to react in a specified in the Shutdown on allocated audit storage manner when the allocated audit storage in the	
Time Alerts allocated audit storage space is full. A conform TOE may support the enforcement of this control, depending on behavior specified in the ST and the assignment chosen for this control AU-5(4) Response to Audit Processing Failures: Shutdown on allocated audit storage space is full. A conformat TOE has ability to react in a specified in the shutdown on allocated audit storage space.	
space is full. A conform TOE may support the enforcement of this control, depending on behavior specified in th ST and the assignment chosen for this control AU-5(4) Response to Audit Processing Failures: Shutdown on allocated audit storage	
TOE may support the enforcement of this control, depending on behavior specified in the ST and the assignment chosen for this control AU-5(4) Response to Audit Processing Failures: Shutdown on AU-5(4) AU-5(4) Response to Audit Processing Failures: Shutdown on Audit Storage	
AU-5(4) Response to Audit Processing Failures: Shutdown on enforcement of this control, depending on behavior specified in th ST and the assignment chosen for this control A conformant TOE has ability to react in a spe	ant
AU-5(4) Response to Audit Processing Failures: Shutdown on Control, depending on behavior specified in the ST and the assignment chosen for this control AU-5(4) Response to Audit Processing Failures: Shutdown on Audit Storage	
behavior specified in the ST and the assignment chosen for this control AU-5(4) Response to Audit Processing Failures: Shutdown on allocated audit storage	
AU-5(4) Response to Audit Processing Failures: Shutdown on ST and the assignment chosen for this control A conformant TOE has ability to react in a spe	the
AU-5(4) Response to Audit Processing Failures: Shutdown on Aconformant TOE has ability to react in a spe	e
AU-5(4) Response to Audit Processing Failures: Shutdown on A conformant TOE has ability to react in a speemanner when the allocated audit storage	;
Audit Processing ability to react in a spe Failures: manner when the Shutdown on allocated audit storage	
Audit Processing ability to react in a spe Failures: manner when the Shutdown on allocated audit storage	the
Shutdown on allocated audit storage	cific
Failure space is full. A conform	ant
TOE may support the	
enforcement of this	
control, depending on	the
behavior specified in the	ie
ST and the assignment	;
chosen for this control	
AU-9 Protection of A conformant TOE has	the
Audit Information ability to prevent	
unauthorized modifica	ion
and deletion of audit	
records.	
AU-9(2) Protection of A conformant TOE mus	t be
Audit able to transmit audit of	lata
Information: to a logically remote	
Audit Backup on location. It can be used	to
Separate Physical support the enforcement	
Systems / of this control if the	nt
Components recipient of the audit d	nt
is physically remote fro	
the TOE.	ata

FCS_CKM.1	Cryptographic Key	SC-12	Cryptographic	The ability of the TOE to
TC3_CKIVI.1	Generation Generation	30-12		generate asymmetric keys
	Generation		Key Establishment	satisfies the key generation
				, -
			and Management	portion of this control.
		SC-12(3)	Cryptographic	A conformant TOE ensures
			Key	that generated asymmetric
			Establishment	keys provide an
			and	appropriate level of
			Management:	security.
			Asymmetric Keys	
FCS_CKM.2	Cryptographic Key	SC-12	Cryptographic	A conformant TOE
	Establishment		Key	supports this control by
			Establishment	providing a key
			and Management	establishment function.
		SC-12(3)	Cryptographic	A conformant TOE
		, ,	Key	supports the production of
			Establishment	asymmetric keys by
			and	providing a key
			Management:	establishment function.
			Asymmetric Keys	
FCS_CKM.4	Cryptographic Key	SC-12	Cryptographic	A conformant TOE has the
TC5_CKWI.4	Destruction Rey	30 12	Key	ability to securely destroy
	Destruction		Establishment	cryptographic keys.
			and Management	cryptograpine keys.
FCS_COP.1/	Cryptographic	SC-13	Cryptographic	A conformant TOE has the
_		3C-13	Protection	ability to perform
DataEncryption	Operation (AES Data		Protection	symmetric encryption and
	Encryption/			decryption using NSA-
	<u>Decryption)</u>			approved and FIPS-
				validated algorithms.
FCS_COP.1/SigGen	Cryptographic	SC-13	Cryptographic	A conformant TOE has the
	Operation (Signature		Protection	ability to perform
	Generation and			cryptographic signing using
	Verification)			NSA-approved and FIPS-
	,			validated algorithms.
FCS_COP.1/Hash	Cryptographic	SC-13	Cryptographic	A conformant TOE has the
1 65_661.1/110311	Operation (Hash	36 13	Protection	ability to perform
	Algorithm)		Trotection	cryptographic hashing
	Aigoritiiiij			using NSA-approved and
				FIPS-validated algorithms.
FCC COD 1/	Countaguaphia	56.12	Counte anamhia	A conformant TOE has the
FCS_COP.1/	Cryptographic	SC-13	Cryptographic	ability to perform keyed-
KeyedHash	Operation (Keyed		Protection	hash message
	Hash Algorithm)			authentication using
				NSA-approved and FIPS-
				validated algorithms.
ECC DDC EVT 1	Pandom Pit	SC-12	Cruntographic	A conformant TOE's use of
FCS_RBG_EXT.1	Random Bit	3C-12	Cryptographic	
			OV	
	<u>Generation</u>		Key	an appropriate DRBG ensures that generated

			Establishment	keys provide an
			and Management	appropriate level of
			and Management	
FIA AFI 4	A	46.7	11	security.
FIA_AFL.1	Authentication	AC-7	Unsuccessful	The TOE has the ability to
	Failure Management		Logon Attempts	detect when a defined
				number of unsuccessful
				authentication attempts
				occurs and take some
				corrective action.
FIA_PMG_EXT.1	<u>Password</u>	IA-5(1)	Authenticator	A conformant TOE will
	<u>Management</u>		Management:	have the ability to enforce
			Password-Based	some minimum password
			Authentication	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	AC-14	Permitted Actions	A conformant TOE will
LIM_OIM_EXT.1	and Authentication	AC-14	Without	define a list of actions that
	and Authentication		Identification or	
				are permitted prior to
		14.2	Authentication	authentication.
		IA-2	Identification and	A conformant TOE has the
			Authentication	ability to require that
			(Organizational	certain functions require successful authentication
			Users)	to access.
FIA_UAU_EXT.2	Password-Based	IA-5(1)	Authenticator	A conformant TOE will
TIA_OAO_EXT.2	Authentication	1/2-2(1)	Management:	have the ability to
	<u> </u>		Password-Based	authenticate users with a
			Authentication	
				password-based authentication mechanism.
FIA 11A11.7	Durate start	14.6	A 4 la 4 la	
FIA_UAU.7	<u>Protected</u>	IA-6	Authenticator	The TOE is required to
	<u>Authentication</u>		Feedback	provide obscured feedback
	<u>Feedback</u>			to the user while
				authentication is in
	-			progress.
FMT_MOF.1/	Management of	AC-3	Access	A conformant TOE will not
ManualUpdate	Security Functions		Enforcement	permit application of a
	<u>Behavior</u>			TOE update unless proper
				authorization is provided.
		AC-3(7)	Access	A conformant TOE will
			Enforcement:	restrict access to
			Role-Based Access	management functionality
			Control	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.

EDT CVD EVT 1	Ductoction of TCF	CC 12	Cmmtaguardia	A conformant TOE
FPT_SKP_EXT.1	Protection of TSF	SC-12	Cryptographic	supports the enforcement
	<u>Data</u>		Key	of this control by
			Establishment	protecting stored
			and Management	cryptographic data. If that
				cryptographic data. If that
				includes authentication
				data, it supports IA-5 part
				(h) as well.
FPT TST EXT.1	TSF Testing	SI-6	Security Function	A conformant TOE will run
			Verification	automatic tests to ensure
				correct operation of its
				own functionality.
		SI-7	Software,	One of the self-tests the
		31-7	Firmware, and	TOE may perform is an
			Information	integrity test of its own
				software or firmware.
EDT TUD EVT 4		014.5(0)	Integrity	
FPT_TUD_EXT.1	Trusted Update	CM-5(3)	Access	A conformant TOE
			Restrictions for	requires that updates to
			Change: Signed	it include integrity
			Components	measures. Depending on
				the selection made in the
				SFR, this may include a
				digital signature.
		SI-7(1)	Software,	A conformant TOE has the
			Firmware and	ability to verify the
			Information	integrity of updates to it.
			Integrity: Integrity	
			Checks	
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:	A conformant TOE may
		` '	Synchronization	have the ability to
		1	with Authoritative	synchronize with an
			Time Source	NTP server in its
				operational environment,
		1		satisfying this control.
FTA_SSL_EXT.1	TSF-Initiated Session	AC-11	Session Locking	A conformant TOE may
	Locking			have the ability to lock an
		1		idle local interactive
				session, depending on the
				selection made in the SFR.
		AC-12	Session	A conformant TOE may
		AC-12		have the ability to
			Termination	terminate an idle local
				interactive session,
		1	I .	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	<u>User-Initiated</u> <u>Termination</u>	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 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 or	A conformant TOE will have the ability to prevent unauthorized disclosure of information and detect

			Alternate Physical	
			Protection	modification to that
		60.11		information.
		SC-11	Trusted Path	The TOE establishes a
				trusted communication
				path between remote
				users and itself.
Optional Requirements		.		
FAU_STG.1	Protected Audit Trail	AU-9	Protection of	A conformant TOE has the
	<u>Storage</u>		Audit Information	ability to prevent
				unauthorized modification
				and deletion of audit
				records.
		AU-9(6)	Protection of	A conformant TOE has the
			Audit	ability to prevent
			Information: Read	unauthorized modification
			Only Access	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/	Counting Lost Audit	AU-5	Response to	A conformant TOE has the
LocSpace	Data		Audit Processing	ability to count the
2000 000			Failures	amount of audit data that
			- and co	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
EALL STC 2/	Action in Case of	ALLE	Posnovas ta	part (b) of the control. A conformant TOE will
FAU_STG.3/	Action in Case of Possible Audit Data	AU-5	Response to	have the ability to
LocSpace	Loss		Audit Processing	generate a warning if local
	<u> </u>		Failures	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	A conformant TOE will
			Audit Processing	have the ability to
			Failures: Audit	generate a warning if local
			Storage Capacity	audit storage space is
		AU-5(1)	Audit Processing	qualifies as an 'alert.' A conformant TOE will have the ability to

				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/	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.
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	A conformant TOE will use cryptographic methods to protect data in transit

			Alternate Physical Protection	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.
Selection-Based Requ	irements			
FAU_GEN_EXT.1	Security Audit 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 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

AU-3(1) Content of Audit Records: Additional Audit Information that is required by FAU_GEN.1.2, Information Individual TOE component that generates each audit uniquely identify the individual TOE component that generates each audit record. AU-12 Audit Generation AU-12 Audit Generation A conformant TOE supports the enforcement of this control by having each of its distributed
AU-3(1) Content of Audit Records: Additional Audit 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 Generation A conformant TOE supports the enforcement of this control by having
AU-3(1) Content of Audit Records: Additional Audit 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 Generation A conformant TOE supports the enforcement of this control by having
Records: Additional Audit required by FAU_GEN.1.2, a conformant TOE will uniquely identify the individual TOE component that generates each audit record. AU-12 Audit Generation A conformant TOE supports the enforcement of this control by having
Additional Audit required by FAU_GEN.1.2, a conformant TOE will uniquely identify the individual TOE component that generates each audit record. AU-12 Audit Generation A conformant TOE supports the enforcement of this control by having
Information Information a conformant TOE will uniquely identify the individual TOE component that generates each audit record. AU-12 Audit Generation A conformant TOE supports the enforcement of this control by having
uniquely identify the individual TOE component that generates each audit record. AU-12 Audit Generation A conformant TOE supports the enforcement of this control by having
individual TOE component that generates each audit record. AU-12 Audit Generation A conformant TOE supports the enforcement of this control by having
AU-12 Audit Generation A conformant TOE supports the enforcement of this control by having
AU-12 Audit Generation A conformant TOE supports the enforcement of this control by having
AU-12 Audit Generation A conformant TOE supports the enforcement of this control by having
supports the enforcement of this control by having
of this control by having
of this control by having
l
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.3 Protected Local Audit AU-4 Audit Storage A conformant TOE
Event Storage for Distributed TOEs Capacity 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 assignment chosen for the control.
Failures distributed components to react in a specific manner
when the allocated audit
storage space for a
component is full.
Depending on the actions
taken by the TOE when thi
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 A conformant TOE has the
Audit Processing ability to react in a specific

	1			
			Failures: Real-	manner when the
			Time Alerts	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	A conformant TOE has the
		, ,	Audit Processing	ability to react in a specific
			Failures:	manner when the
			Shutdown on	allocated audit storage
				space for one of its
			Failure	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.4	Protected Remote	AU-4(1)	Audit Storage	A conformant TOE has the
1A0_510_EX1.4	Audit Event Storage	A0-4(1)	Capacity: Transfer	ability to buffer local audit
	for Distributed TOEs		to Alternate	records on its distributed
	ioi Distributed TOLS		Storage	components until this data
			Storage	is transferred to a central
				component that is used for
				storing audit records.
		AU-9	Protection of	A conformant TOE has the
		A0-3	Audit Information	ability to prevent
			Audit information	unauthorized modification
				and deletion of buffered
				audit records that reside
				on distributed components
				while awaiting transfer to a
				centralized location.
		AU-9(2)	Protection of	A conformant TOE must be
		A0-3(2)		able to transmit audit data
			Audit	from distributed
			Information:	components to a
			Audit Backup on	centralized component on
			Separate Physical	another part of the TOE. It
			Systems /	can be used to support the
			Components	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

	1	1		I 6.1.1
				of this control if
				centralization of data from
				distributed components is
				an intermediate step in
				satisfying FAU_STG_EXT.1.
		AU-12(1)	Audit Generation:	A conformant TOE will
		/10(_/	System-Wide /	consolidate the audit logs
			Time-Correlated	from its distributed
			Audit Trail	
			Audit ITali	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	The TOE supports a
			Confidentiality	cryptographic method of
			and Integrity:	protecting data in transit
			Cryptographic or	between its distributed
			Alternate Physical	components.
			Protection	Somponemen
FCS_DTLSC_EXT.1	DTLS Client Protocol	IA-5(2)	Authenticator	The TOE requires peers to
1 C3_D1 C3C_EXT.1	DTES CHERT TTOCOCOL	", 3(2)	Management:	possess a valid certificate
			PKI-Based	before establishing trusted
			Authentication	communications,
			Authentication	supporting this control.
		SC-8	Transmission	A conformant TOE has the
		3C-8		
			Confidentiality	ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted IT
				product.
		SC-8(1)	Transmission	The TOE supports a
			Confidentiality	cryptographic method of
			and Integrity:	protecting data in transit.
			Cryptographic or	
			Alternate Physical	
			Protection	
		SC-13	Cryptographic	The TOE provides
			Protection	cryptographic methods to
				secure data in transit,
				which may satisfy
				organization-defined uses
				if the functionality claimed
				by the TSF is consistent
				with organizational
FCC DTICC EVT 3	DTI C Client Duete - 1	IA F/3\	A th = t =	requirements.
FCS_DTLSC_EXT.2	DTLS Client Protocol	IA-5(2)	Authenticator	The TOE requires peers to
	<u>– with</u>		Management:	possess a valid certificate
	<u>Authentication</u>		PKI-Based	before establishing trusted
			Authentication	communications and
				provides its own client

	1			
				certificate to the peer,
				supporting this control.
		SC-8	Transmission	A conformant TOE has the
			Confidentiality	ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted IT
				product.
		SC-8(1)	Transmission	The TOE supports a
			Confidentiality	cryptographic method of
			and Integrity:	protecting data in transit.
			Cryptographic or	
			Alternate Physical	
		56.42	Protection	The TOE manifeles
		SC-13	Cryptographic	The TOE provides
			Protection	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.
ECC DTICC EVT 1	DTI C Corver Drotocol	IA-5(2)	Authenticator	The TOE provides a
FCS_DTLSS_EXT.1	DTLS Server Protocol	IA-3(2)	Management:	
			PKI-Based	server certificate to a TLS
			Authentication	client before establishing
			Additerritication	trusted communications,
				supporting this control
		SC-8	Transmission	A conformant TOE has the
			Confidentiality	ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted IT
				product.
		SC-8(1)	Transmission	The TOE supports a
			Confidentiality	cryptographic method of
			and Integrity:	protecting data in transit.
			Cryptographic or	
			Alternate Physical	
		56.42	Protection	TI TOE : I
		SC-13	Cryptographic	The TOE provides
			Protection	cryptographic methods to
				secure data in transit,
	i e			which may satisfy
				organization-defined uses
				organization-defined uses if the functionality claimed
				if the functionality claimed
				if the functionality claimed by the TSF is consistent

FCS_DTLSS_EXT.2	DTLS Server Protocol with Mutual Authentication	IA-5(2)	Authenticator Management: PKI-Based Authentication Transmission Confidentiality and Integrity	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. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT
		SC-8(1)	Transmission Confidentiality and Integrity: Cryptographic or Alternate Physical Protection	product. 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
500 ID050 5VT 4		14.5(0)		requirements.
FCS_IPSEC_EXT.1	IPsec Protocol	IA-5(2)	Authenticator	A conformant TOE
			Management: PKI-Based	implements peer
			Authentication	authentication for IPsec.
		SC-7(5)	Boundary	A conformant TOE's IPsec
		(5)	Protection: Deny	implementation includes a
			by Default/Allow	default-deny posture in its
			by Exception	SPD.
		SC-8	Transmission	A conformant TOE
			Confidentiality	implements IPsec as a
			and Integrity	method of ensuring
				confidentiality and
				integrity of data in transit.
		SC-8(1)	Transmission	The TOE's use of IPsec
			Confidentiality	provides a cryptographic
			and Integrity:	means to protect data in
			Cryptographic or	transit.
			Alternate Physical	
		60.10	Protection	TI TOS 11
		SC-13	Cryptographic	The TOE provides
			Protection	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	AU-8(1)	Time Stamps:	A conformant TOE
			Synchronization	supports the enforcement
			with Authoritative	of part (a) of this control by providing a mechanism
			Time Source	to obtain time data from
			Time Source	an authoritative NTP
				server. This SFR does not
				discuss drift correction so
				it is not applicable to part
				(b) of this control
		AU-8(2)	Time Stamps:	This SFR provides a
			Secondary	mechanism to support the
			Authoritative	enforcement of this
			Time Source	control by requiring the
				TSF to support multiple
				separate NTP servers as

		SC-8	Transmission Confidentiality and Integrity	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. 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.
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 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 asneeded 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 Cryptographic Protection	The TOE's use of SSH supports a cryptographic method of protecting data in transit. 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	IA-2	Remote Access: Protection of Confidentiality / Integrity Using Encryption Identification and Authentication (Organizational Users)	The SSH client protocol implemented by the TOE provides confidentiality and integrity for remote access. A conformant TOE provides SSH server functionality that enforces identification and authentication of organizational users attempting to access the TSF.
		SC-8(1)	Transmission Integrity Transmission Confidentiality and Integrity: Cryptographic or Alternate Physical	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE's use of SSH enforces 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.1	TLS Client Protocol	IA-5(2)	Authenticator	The TOE requires peers to
TCS_TESC_EXT.1	113 CHERT PROTOCOL	IA-3(2)	Management:	possess a valid certificate
			PKI-Based	before establishing trusted
			Authentication	communications,
				supporting this control.
		SC-8	Transmission	A conformant TOE has the
			Confidentiality	ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted IT
				product.
		SC-8(1)	Transmission	The TOE supports a
		, ,	Confidentiality	cryptographic method of
			and Integrity:	protecting data in transit.
			Cryptographic or	1
			Alternate Physical	
			Protection	
		SC-13	Cryptographic	The TOE provides
			Protection	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	IA-5(2)	Authenticator	The TOE requires peers to
1.00_1.00_2.	with Authentication	" (3(2)	Management:	possess a valid certificate
	with Addientication		PKI-Based	before establishing trusted
			Authentication	communications and
				provides its own client
				certificate to the peer,
				supporting this control.
		SC-8	Transmission	A conformant TOE has the
			Confidentiality	ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted IT
				product.
		SC-8(1)	Transmission	The TOE supports a
			Confidentiality	cryptographic method of
			and Integrity:	protecting data in transit.
			Cryptographic or	
			Alternate Physical	
		CC 13	Protection	The TOE was dele-
		SC-13	Cryptographic	The TOE provides
			Protection	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	The TOE provides a server
			Management: PKI-Based Authentication	certificate to a TLS client before establishing trusted communications, supporting this control.
		SC-8	Transmission	A conformant TOE has the
			Confidentiality	ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted IT
				product.
		SC-8(1)	Transmission	The TOE supports a
			Confidentiality	cryptographic method of
			and Integrity: Cryptographic or	protecting data in transit.
			Alternate Physical	
			Protection	
		SC-13	Cryptographic	The TOE provides
			Protection	cryptographic methods to
				secure data in transit,
				which may satisfy
				organization-defined uses
				if the functionality claimed
				by the TSF is consistent
				with organizational
FOR THE EVE 2	TIC Common Durata and	14 5/2)	Authorists:	requirements.
FCS_TLSS_EXT.2	TLS Server Protocol with Mutual	IA-5(2)	Authenticator Management:	The TOE requires peers to possess a valid certificate
	Authentication		PKI-Based	before establishing trusted
	Authentication		Authentication	communications and
				provides its own server
				certificate to the peer,
				supporting this control.
		SC-8	Transmission	A conformant TOE has the
			Confidentiality	ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted IT
				product.

	1	00.0(1)	1	
		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.
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.

	T	1000(7)	T .	
		AC-3(7)	Access	A conformant TOE will
			Enforcement:	restrict access to
			Role-Based Access	management functionality
			Control	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/	Management of TSF	AC-3	Access	A conformant TOE will not
CryptoKeys	Data	7.00	Enforcement	permit manipulation of
Cryptokeys	Data		Emorcement	cryptographic data unless
				proper authorization is
		(=)	1_	provided.
		AC-3(7)	Access	A conformant TOE will
			Enforcement:	restrict access to
			Role-Based Access	management functionality
			Control	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_TST_EXT.2	Self-Tests Based on	SI-7	Software,	A conformant TOE
	Certificates		Firmware, and	supports the enforcement
	<u>certificates</u>		Information	of this control by using a
				· -
			Integrity	Code Signing certificate as
				a method of integrity
				verification.
		SI-7(1)	Software,	A conformant TOE
			Firmware, and	supports the enforcement
			Information	of this control by using a
			Integrity: Integrity	Code Signing certificate to
			Checks	verify the TOE's
				software/firmware
				integrity.
		SI-7(12)	Software,	A conformant TOE
		',	Firmware, and	supports the enforcement
			Information	of this control by providing
		1	Integrity: Integrity	a mechanism to verify the
			Verification	integrity of installed
			VEITHCALION	software updates.
EDT TUD EVT 2	Tructod Undetes	CM-5(3)	Access	A conformant TOE
FPT_TUD_EXT.2	Trusted Updates	Civi-3(3)		
	Based on Certificates	1	Restrictions for	supports the enforcement
			Change: Signed	of this control by using
		1	Components	code signing certificates
		1		for software updates.
		SI-7(15)	Software,	A conformant TOE's use of
			Firmware, and	a code signing certificate
	1			

			Information Integrity: Code Authentication	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.