TEs in Pink have been added & TEs in Green have been kept from FIPS 140-2 regression test (deleted/removed TEs from FIPS 140-2 are not included/marked)

Regression Testing Table

AS	TE	Security Level				Conditional Testing	TEs Notes	Scenarios				FIPS-140-3/ ISO TE definition
		1	2	3	4			OEUP, PTSC, UPDT	TRNS – Code Change	TRNS – No Code Change	CVEs	
Section 6.2 - Cryptographic Module Specification												
AS02.13	TE02.13.02	x	x	x	x	Excluded Components	ADDED (140-2: TE01.09.01)	x				The tester shall verify the correctness of any rationale for **exclusion** provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed.
	TE02.13.03	x	x	x	x	Excluded Components	ADDED	x				The tester shall manipulate (e.g. to cause the component to operate not as designed) the **excluded components** in a manner to cause incorrect operation of the excluded component. The tester shall verify that the incorrect operation of the excluded component shall not interfere with the approved secure operation of the module.
AS02.19	TE02.19.02	x	x	x	x		(140-2: TE01.03.02)	x	x	x	x	The tester shall invoke the approved mode of operation using the vendor provided instructions found in the non-proprietary security policy. The tester shall verify, by inspection and from the vendor documentation, that the cryptographic module is the approved mode of operation as a result of documented instructions.
AS02.20	TE02.20.01	x	x	x	x		ADDED (140-2: TE01.12.01)	x	x	x	x	The tester shall verify that the vendor has provided a **validation certificate for each approved security function** issued by a validation authority.
	TE02.20.02	x	x	x	x		ADDED (140-2: TE01.12.02)	x	x	x		The tester shall verify that the vendor has provided **the list of non-approved security functions.**
AS02.21	TE02.21.01	x	x	x	x		ADDED (No 140-2)	x	x	x		The tester shall verify by inspection that the vendor provided documentation identifies all of non-approved cryptographic algorithms, security functions or processes utilized for each service in each approved mode of operation.
	TE02.21.02	x	x	x	x		ADDED (No 140-2)	x	x	x		The tester shall verify the correctness of any rationale provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed.
AS02.22	TE02.22.02	x	x	x	x		ADDED (No 140-2)	x	x	x		The tester shall verify by inspection and from the vendor documentation that the CSPs are exclusive between approved and non-approved services and modes of operation.
AS02.24	TE02.24.02	x	x	x	x		ADDED (No 140-2)	x	x	x	x	The tester shall execute all services and verify that the indicator provides an unambiguous indication of whether the service utilizes an approved security function or process in an approved manner or not.
AS02.26	TE02.26.03	x	x	x	x	Degraded Operation	ADDED (No 140-2)	x				The tester shall exercise the cryptographic module, causing it to operate in each degraded operation. For each degraded operation, the tester shall attempt to perform a service to verify that all conditional algorithm self-tests are performed prior to the first operational use of any cryptographic algorithm.
	TE02.26.04	x	x	x	x	Degraded	ADDED	x				The tester shall first exercise the cryptographic module, causing it to operate in each degraded operation. The tester shall next perform pre-operational self-tests to verify that the cryptographic module remains in degraded operation

						Operation	(No 140-2)					until such time the cryptographic module passes without failure all pre-operational self-tests successfully.
	TE02.26.05	x	x	x	x	Degraded Operation	ADDED (No 140-2)	x				The tester shall first exercise the cryptographic module, causing it to operate in each degraded operation. The tester shall next perform pre-operational self-tests, causing an error condition in pre-operational self-tests to occur. The tester shall verify that the cryptographic module does not remain in degraded operation but enters an error state.
AS02.30	TE02.30.02	x	x	x	x	Degraded Operation	ADDED (No 140-2)	x				The tester shall exercise the cryptographic module and verify that the documented indicator is provided if attempts are made to use a non-functioning security function, or process.
Section 6.3 - Cryptographic Module Interfaces												
AS03.07	TE03.07.02	x	x	x	x		(140-2: TE02.06.02)	x	x		x	The tester shall cause the cryptographic module to enter each of following states: a) a state performing manual SSP entry; b) a self-test state performing pre-operational self-tests; c) a state performing software/firmware load test; d) a state performing zeroisation; e) an error state; and verify that all data output via the data output interface is inhibited.
AS03.10	TE03.10.02	x	x	x	x	Control Output	ADDED (No 140-2)	x	x		x	The tester shall cause the cryptographic module to enter each specified error state and verify that all control output via the control output interface is inhibited. If status information is output from the status output interface to identify the type of error, the tester shall verify that the information output is not sensitive. The following actions may be used to cause the cryptographic module to enter an error state — opening a tamper-detecting cover or door, entering incorrectly-formatted commands, keys, or parameters, reducing input voltage, and/or any other error-causing actions. If it is not possible for the tester to cause an error, then the vendor shall provide a rationale to the tester why this test cannot be performed.
AS03.15	TE03.15.05	x	x	x	x		ADDED (No 140-2)	x	x			The tester shall examine the applicable source code(s) to ensure that the identified component is actually validating the documented format.
	TE03.15.06	x	x	x	x	For TRNS: Input data and/or control information associated with transitioning algorithm	ADDED (No 140-2)	x	x			The tester shall attempt to input data and/or control information which is not compliant with the format, and verify that such service inputs are rejected by the cryptographic module. NOTE The test platform or configuration can impose a part of format/restrictions. EXAMPLE 1 A device driver to use the cryptographic module is enforcing a part of the format. EXAMPLE 2 A layer in a protocol stack supports fixed length packet only.
AS03.18	TE03.18.02			x	x	Physical Trusted Channel	(140-2: TE02.16.02)	x				If the cryptographic module inputs or outputs plaintext CSPs, the tester shall verify that only plaintext CSPs enter or exit the module through the applicable physical ports, and that no other data, plaintext or encrypted, enters or exits the module via the applicable physical ports.
AS03.19	TE03.19.02			x	x	Logical Trusted Channel	(140-2: TE02.17.02)	x				If the cryptographic module inputs or outputs plaintext CSPs, the tester shall verify that plaintext CSPs enter or exit the module through the applicable logical interface using the trusted channel, and that no other data, plaintext or encrypted, enters or exits the module via the applicable logical interface using the trusted channel.
	TE03.19.04			x	x		(140-2:	x				The tester shall, by attempting to access the communication link, verify that the trusted channel prevents

							TE06.22.03)					unauthorised modification, substitution, and disclosure along the communication link.
Section 6.4 – Roles, services and authentication												
AS04.02	TE04.02.02	x	x	x	x		(140-2: TE03.02.02)	x				The tester shall assume the identity of two independent operators: Operator1 and Operator2. The operators shall assume different roles. The tester shall verify that only the services allocated to each role can be performed in that role. The tester shall also attempt, for each operator, to access services that are unique to the role assumed by the other operator in order to verify that separation is maintained between the roles and services allowed in concurrent operators.
AS04.07	TE04.07.03	x	x	x	x	Maintenance	ADDED (140-2: TE03.05.03)	x				While in the maintenance role, the tester shall enter, for all unprotected SSPs, known values which are effective in demonstrating the zeroisation and, upon exit from the maintenance role, shall verify that zeroisation has taken place.
AS04.11	TE04.11.02	x	x	x	x	For TRNS or CVE: New/added/ changed services	(140-2: TE03.14.02 TE03.15.02)	x	x	x	x	The tester shall perform the following for each service (i.e. security and non-security services, both approved and non-approved services). — Enter each of the specified service inputs and observe that they result in the specified service outputs. — For services that require the operator to assume a role, the role shall be assumed to enter each of the specified service inputs and observe that they result in the specified service outputs. — For services that require the operator to assume a role, assume the role that is not specified for the service and enter each of the specified service inputs and observe that the service is not provided. — For services that require the operator to assume an authenticated role, the role shall be assumed and authenticated to enter each of the specified service inputs and observe that they result in the specified service outputs. — For services that require the operator to assume an authenticated role, the role shall be assumed but the authentication data shall be modified to fail authentication and enter each of the specified service inputs and observe that the service is not provided. — For services that provide data output over the data output interface, the tester shall verify the result against the expected result.
AS04.13	TE04.13.01	x	x	x	x		ADDED (No 140-2)	x	x	x	x	The tester shall verify that the service outputs (i.e. name or module identifier and versioning information) are consistent with specification and with information provided under assertions AS02.11, AS02.12, and AS11.04.
	TE04.13.02	x	x	x	x		ADDED (No 140-2)	x	x	x	x	The tester shall verify that the vendor provided documentation (i.e. non-proprietary security policy or an Administrator guidance) provides sufficient information to unambiguously identify the module version.
	TE04.13.03	x	x	x	x		ADDED (No 140-2)	x	x	x	x	The tester shall verify that the output of the current name or module identifier and the versioning information is sufficient for an operator to correlate the module with a validation record, with the help of non-proprietary security policy or an administrator guidance.
AS04.20	TE04.20.01	x	x	x	x	Bypass	(140-2: TE03.12.01)	x				The tester shall verify whether the bypass capability is implemented by the module. The tester shall verify the vendor documentation to verify that the bypass capability is allocated to at least one authorized role.
AS04.22	TE04.22.02	x	x	x	x	Bypass	(140-2: TE03.13.02)	x				The tester shall transition **to each bypass state** and verify that the "**Show Status**" indicates the applicable bypass status
AS04.32	TE04.32.01	x	x	x	x	Operator capability – update allowed by user and not	ADDED (No 140-2)	x				The tester shall **initiate the software/firmware** load test. After the pre-operational self-tests

						factory						have been successfully executed subsequent to software/firmware load test, the tester shall verify that **the versioning information is modified** to represent the **addition and/or update of the newly loaded software or firmware.**
AS04.35	TE04.34.01	x	x	x	x	Complete image replacement	ADDED (No 140-2)	x				The tester shall initiate the software/firmware load test. After the software/firmware load test passed, the tester shall verify that the loaded software or firmware cannot be used until after the pre-operational self-tests have been successfully executed through power-on reset.
AS04.35	TE04.35.02	x	x	x	x	Complete image replacement	ADDED (No 140-2)	x				The tester shall note which **SSPs are present** in the module and initiate the power-on reset subsequent to **software/firmware load test.** Following the completion of the pre-operational self-test, the tester shall attempt to perform cryptographic operations using each of the SSPs that were stored in the module prior to execution of the new image. The tester shall verify that each **SSP cannot be accessed.**
AS04.37	TE04.37.02		x	x	x		(140-2: TE03.17.02)	x				The tester shall assume each role and initiate an error during the authentication procedure. The tester shall verify that the module denies access to each role.
AS04.38	TE04.38.02		x	x	x		(140-2: TE03.18.02)	x				The tester shall perform the following tests: -Assume a role, attempt to modify to another role that the operator is authorised to assume, and verify that the module allows the operator to request services assigned to the new role. -Assume a role, attempt to modify to another role that the operator is not authorised to assume, and verify that the module does not allow the operator to request the services assigned only to the new role.
AS04.39	TE04.39.02			x	x		ADDED (No 140-2)	x				The tester shall verify by inspection and from the vendor documentation that the identification and authentication procedure is implemented as specified in the vendor documentation provided under VE04.39.01.
	TE04.39.03			x	x		(140-2: TE03.19.03)	x				The tester shall initiate an error during the authentication procedure and shall verify that the module does not allow the tester to proceed beyond the authentication procedure.
	TE04.39.04			x	x		ADDED (No 140-2)	x				The tester shall successfully authenticate his/her identity to the module. When required to select one or more roles, the tester shall select roles not compatible with the authenticated identity and shall verify that authorization to assume the roles is denied. NOTE 11 This test procedure is associated with AS04.39 and AS04.41.
AS04.42	TE04.42.03			x	x		ADDED (No 140-2)	x				The tester shall perform the following tests. a) Assume each role, attempt to modify to another role that the tester is authorized to assume, verify that the tester's identity does not have to be reauthenticated, and verify that the tester can access the services associated with the new role. The tester shall perform services in the new role that were not associated with the previous role in order to verify that the tester has assumed a different role. b) Assume each role, attempt to modify to another role that the operator is not authorized to assume, and verify that the module denies access to the role based on the identity of the operator.
	TE04.42.04			x	x		ADDED (No 140-2)	x				The tester shall exercise the cryptographic module and verify that the changing to a Crypto Officer role from any other role other than the Crypto Officer role is prohibited as specified in the vendor documentation provided under VE04.42.01.
AS04.43	TE04.43.02		x	x	x	For TRNS: New/added/ changed services	(140-2: TE03.21.02)	x	x	x		The tester shall authenticate to the module and assume one or more roles, **power off the module, power on the module,** and attempt to perform services in those roles. To meet this assertion, the module shall deny access to the services and require that the **tester be reauthenticated**.
AS04.44	TE04.44.02		x	x	x		ADDED (140-2:	x				The tester shall perform the following tests. a) Attempt to access (by circumventing the documented protection mechanisms) authentication data for which the tester is not authorized to have access. If the module denies access or allows access only to encrypted or otherwise

							TE03.22.02)					protected forms of data, the requirement is met. b) Modify authentication data using any method not specified by the vendor documentation and attempt to enter the modified data. The module shall not allow the tester to be authenticated using the modified data.
AS04.45	TE04.45.03		x	x	x		ADDED (No 140-2)	x				If default authentication data is used to access to the module and to initialize the authentication mechanism, the tester shall assume the authenticated role, and verify that the default authentication data is replaced upon the first-time authentication. The tester shall also enter the default authentication data after the first-time authentication and verify that the cryptographic module does not allow the tester to be authenticated.
Section 6.5 Software/Firmware security												
AS05.05	TE05.05.07	x	x	x	x	Software/Firmware	(140-2: TE06.08.02)	x	x	x	x	(Software/firmware) The tester shall modify the cryptographic software and firmware components. This test is failed if the integrity mechanisms do not detect the modifications.
AS05.06	TE05.06.06	x	x	x	x	Hardware	ADDED (No 140-2)	x	x	x	x	(Hardware) The tester shall modify the cryptographic software and firmware components. This test is failed if the integrity mechanisms do not detect the modifications.
AS05.08	TE05.08.02	x	x	x	x	Software/Firmware	ADDED (No 140-2)	x				The tester shall verify that any temporary values generated during the integrity test are zeroised upon completion of the integrity test.
AS05.15	TE05.15.02		x	x	x		ADDED (No 140-2)	x	x	x	x	The tester shall verify, by inspection and from the vendor documentation, that the documented executable form is used for each software/firmware components.
AS05.17	TE05.17.02		x	x	x	Software/Firmware	ADDED (No 140-2)	x				The tester shall attempt to corrupt the cryptographic software and firmware components. If the module determines that the integrity is maintained, this test is failed.
Section 6.6 - Operational Environment												
AS06.05	TE06.05.03	x	x				(140-2: TE06.05.01)	x				The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are executing, the same or another tester shall attempt to gain unauthorized access to secret and private keys, intermediate key generation values, and other SSPs which are under the control of the cryptographic module.
AS06.06	TE06.06.02	x	x				ADDED (No 140-2)	x				The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are executing, the same or another tester shall attempt to gain access to CSPs and perform modifications of SSPs regardless if this data is in the process memory or stored on persistent storage within the operational environment. **Note: should be able to test TE06.06.02 and .06.08.03 at the same time**
AS06.08	TE06.08.03	x	x				ADDED (No 140-2)	x				The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are executing, the same or another tester shall attempt to gain ownership of a spawned cryptographic process that is owned by a cryptographic module from either a separate external process or operator. **Note: should be able to test TE06.06.02 and .06.08.03 at the same time**
AS06.10	TE06.10.03		x				ADDED (No 140-2)	x				The tester shall configure the operating systems role-based access controls or discretionary access controls to give permissions to a specific user or group. The tester, assuming a different user or group role, shall attempt to execute, modify, or read SSPs, control or status data which the tester has unauthorized access.
AS06.11	TE06.11.03		x				ADDED (No 140-2)	x				The tester shall configure the operating system to protect against unauthorized execution, modification, and reading of SSPs, control and status data. During execution of a cryptographic process, the tester shall attempt to execute, modify or read SSPs, control or status data which the tester has unauthorized access.

AS06.12	TE06.12.02		x				(140-2: TE06.11.02)	x				The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to give exclusive rights to execute the stored cryptographic software. The tester shall verify that they have exclusive rights to execute the stored cryptographic software.
AS06.13	TE06.13.02		x				(140-2: TE06.12.02)	x				The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to give exclusive rights to execute the stored cryptographic software. The tester shall verify that they have exclusive rights to modify (i.e., write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data.
AS06.14	TE06.14.02		x				(140-2: TE06.13.03)	x				The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to give exclusive rights to read cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data.
AS06.15	TE06.15.02		x				(140-2: TE06.14.02)	x				The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to **give exclusive rights to *enter* SSPs**.
AS06.18	TE06.18.03		x				ADDED (No 140-2)	x				The tester shall configure the operating system control mechanisms to prevent processes in user roles or user groups from gaining either read or write access to SSPs owned by other processes and to system SSPs. The tester shall verify that running processes in user roles or user groups are prevented from gaining either read or write access to SSPs owned by other processes and to system SSPs.
AS06.26	TE06.26.02		x				(140-2: TE06.17.02)	x				The tester shall execute the modules services that provide audit event records and examine the operating system audit logs to verify that the events in AS06.26 {modifications, accesses, deletions, and additions of cryptographic data and SSPs; attempts to provide invalid input for Crypto Officer functions; addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by the cryptographic module); the use of a security-relevant Crypto Officer function; requests to access authentication data associated with the cryptographic module; the use of an authentication mechanism (e.g. login) associated with the cryptographic module; and explicit requests to assume a Crypto Officer role} were recorded. NOTE The tester DOES NOT have to test the audit mechanism provided by the operating system and identified by the vendor. Note it would verify that the input is created (AS06.26 implicit tested via the AS06.27)
AS06.27	TE06.27.02		x				(140-2: TE06.25.02)	x				The tester shall execute the cryptographic module's services to verify that the operating system events in AS06.27 *{all operator read or write accesses to audit data stored in the audit trail; access to files used by the cryptographic module to store cryptographic data or SSPs; addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by operational environment); requests to use authentication data management mechanisms; attempts to use the trusted channel function and whether the request was granted, when trusted channel is supported at this security level; and identification of the initiator and target of a trusted channel, when trusted channel is supported at this security level}* were recorded. Note it would verify that the input is created (AS06.26 implicit tested via the AS06.27)
AS06.28	TE06.28.02		x				ADDED (No 140-2)	x				The tester shall configure the operating system controls to prevent operators other than those with the privileges identified in the Security Policy from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.
AS06.28	TE06.28.03		x				ADDED (No 140-2)	x				The tester shall assume the privileges identified in the Security Policy to allow modification of the cryptographic module software and audit data stored within the operational environment of the cryptographic module and verify that modification can be achieved.
AS06.28	TE06.28.03		x				ADDED (No 140-2)	x				The tester shall assume the privileges identified in the Security Policy that do not allow modification of the cryptographic module software and audit data stored within the operational environment of the cryptographic

												module and verify that modification cannot be achieved.
Section 6.7 Physical Security												
	None											
Section 6.8 Non-Invasive Security												
	None											
Section 6.9 - Sensitive Security Parameter Management												
AS09.01	TE09.01.02	x	x	x	x	For TRNS: CSPs associated with the transitioning algorithm	(140-2: TE07.01.02)	x	x			The tester shall attempt to access (by circumventing the documented protection mechanisms) CSPs for which the tester is **not authorised to** access. To meet this assertion the module is required to deny access.
AS09.01	TE09.01.03	x	x	x	x	For TRNS: CSPs associated with the transitioning algorithm	(140-2: TE07.01.02)	x	x			The tester shall attempt to modify CSPs using any method not specified by the vendor documentation. NOTE CSPs encrypted using a non-approved algorithm or proprietary algorithm or method are considered in plaintext form within the scope of this document.
AS09.02	TE09.02.02	x	x	x	x	For TRNS: PSPs associated with the transitioning algorithm	(140-2: TE07.02.02)	x	x			The tester shall attempt to modify all PSPs using any method **not specified by the vendor** documentation documented and shall attempt to enter them into the module.
AS09.03	TE09.03.02	x	x	x	x	SSP inputs. For TRNS: SSPs associated with the transitioning algorithm	(140-2: TE07.25.02)	x	x			For each SSP that can be entered, the tester shall first enter the SSP while assuming the correct entity. The tester shall then verify that entry is not possible when assuming an incorrect entity.
	TE09.03.03	x	x	x	x	SSP outputs. For TRNS: SSPs associated with the transitioning algorithm	(140-2: TE07.25.02)	x	x			For each SSP that can be output, the tester shall first output the SSP while assuming the correct entity. The tester shall then verify that output is not possible when assuming an incorrect entity.
AS09.10	TE09.10.02	x	x	x	x		(140-2: TE07.29.02)	x				The tester shall verify from the vendor provided documentation that the implemented automated SSP establishment methods are compliant with the approved automated SSP establishment methods listed in ISO/IEC 19790:2012, Annex D.
AS09.14	TE09.14.02	x	x	x	x	Direct Enter/input SSP	(140-2: TE07.27.02)	x				The tester shall enter all encrypted SSPs and shall monitor the output interfaces of the module to verify that any resulting plaintext SSP values are not displayed.
AS09.16	TE09.16.03						(140-2: TE02.14.02)	x				The tester shall attempt to output plaintext CSPs without the module performing two independent internal actions. The module shall fail if the module allows the output of plaintext CSPs without two independent internal actions.
AS09.21	TE09.21.02			x	x	Split knowledge key	(140-2: TE07.31.04)	x				The tester shall verify the split knowledge procedure splits the key into multiple key components, with each key component individually sharing no knowledge of the original key.
	TE09.21.03			x	x	Split knowledge	(140-2:	x				The tester shall verify that a subset of the split knowledge components or all components are required to be

						key	TE07.31.04)					entered or output for each key.
AS09.25	TE09.25.02	x	x	x	x		(140-2: TE07.39.02)	x				The tester shall modify the association of key and entity. The tester shall then attempt to perform cryptographic functions as one of the entities and shall verify that these functions fail.
AS09.27	TE09.27.02	x	x	x	x	For TRNS: PSPs associated with the transitioning algorithm	(140-2: TE07.02.02)	x	x			The tester shall assume an unauthorized role and attempt to modify PSPs stored within the module and verify that this attempt fails.
AS09.28	TE09.28.02		x	x	x	For TRNS: SSPs associated with the transitioning algorithm	(140-2: TE07.41.02)	x	x		x	The tester shall verify which SSPs are present in the module and **initiate the zeroise command**. Following **the completion of the zeroise command**, the tester shall attempt to perform cryptographic operations using each of the unprotected SSPs that were stored in the module. The tester shall verify that each unprotected SSP cannot be accessed. NOTE: ISO TE is TE09.30.02
	TE09.28.03		x	x	x	For TRNS: SSPs associated with the transitioning algorithm	(140-2: TE07.41.03)	x	x		x	The tester shall initiate zeroisation and verify the SSP destruction method is performed in a time that is not sufficient to compromise unprotected SSPs. NOTE: ISO TE is TE09.30.03
AS09.36	TE09.36.02				x		ADDED (No 140-2)	x				The tester shall perform the module zeroisation. The test shall attempt to interrupt the zeroisation process to prevent its completion in whole or part.
AS09.37	TE09.37.02				x		ADDED (No 140-2)	x				The tester shall perform the module zeroisation. The tester shall verify that the module has returned to the factory state.
Section 6.10 - Self Tests												
AS10.07	TE10.07.03	x	x	x	x		(140-2: TE09.07.03)	x				The tester shall cause each error condition to occur and shall attempt to clear the error condition. The tester shall verify that actions necessary to clear the error condition are consistent with the vendor documentation. If the tester cannot cause each error condition to occur, the tester shall verify the code listing and or design documentation whether the actions necessary to clear each error condition are consistent with the descriptions in the vendor documentation.
AS10.07	TE10.07.04	x	x	x	x		ADDED (No 140-2)	x	x	x	x	The tester shall verify that all self-tests are performed regardless if the cryptographic module operates in an approved mode or non-approved mode.
AS10.07	TE10.07.05	x	x	x	x		(140-2: TE09.09.02)	x	x	x	x	The tester shall verify by inspection and from the vendor documentation that determination of pass or fail of each self-test is made by the module, without external controls, externally provided input text vectors, expected output results, or operator intervention.
AS10.08	TE10.08.03	x	x	x	x	For TRNS: Self-test / Error state associated with the transitioning algorithm	ADDED (140-2: TE09.09.03)	x	x			The tester shall run each self-test and cause the module to enter every error state. The tester shall compare the observed error indicator with the indicator specified in the vendor documentation. If they are not the same, this test is failed.
AS10.09	TE10.09.03	x	x	x	x	For TRNS: Error	(140-2:	x	x			The tester shall cause the module to enter the error state and verify that any cryptographic operations that the

						state associated with the transitioning algorithm	TE09.05.03)					tester attempts to initiate are prevented.
AS10.10	TE10.10.01	x	x	x	x	For TRNS: Error state associated with the transitioning algorithm	ADDED (No 140-2)	x	x			The tester shall cause an error in a function or algorithm that failed a self-test and initiate a functionality that utilize the function or algorithm and verify that the module cannot utilize this functionality.
	TE10.10.02	x	x	x	x	For TRNS: Self-test associated with the transitioning algorithm	ADDED (No 140-2)	x	x			The tester shall run each self-test and cause the module to enter every error state or a degraded operation. The tester shall exercise the cryptographic module, and verify that the functionality cannot be utilized until the relevant self-test has been repeated and successfully passed.
AS10.11	TE10.11.01	x	x	x	x	Implicit error status	ADDED (No 140-2)	x				The tester shall run each self-test and cause the module to enter every error state. The tester shall verify that the module has entered the error state implicitly through the procedure documented in the non-proprietary security policy.
AS10.12	TE10.12.03			x	x	For TRNS: Self-test associated with the transitioning algorithm	ADDED (No 140-2)	x	x			The tester shall cause the cryptographic module to enter an error state and verify that the module generates the error log, at a minimum, for the most recent error event.
	TE10.12.04			x	x		ADDED (No 140-2)	x				The tester shall access the error log without assuming any authenticated role supported by the cryptographic module. If the error log can be accessed, this assertion fails.
	TE10.12.05			x	x		ADDED (No 140-2)	x				The tester shall exercise the cryptographic module and verify that the error log is protected against unauthorized modification and substitution.
AS10.21	TE10.21.03	x	x	x	x	Bypass	ADDED (No 140-2)	x				The tester shall cause each error condition of the pre-operational bypass test to occur and shall verify that the inhibition of output was performed under TE03.07.01 to TE03.07.05 and TE03.10.01 to TE03.10.05.
	TE10.21.04	x	x	x	x	Bypass	ADDED (No 140-2)	x				The tester shall run the pre-operational bypass test and shall verify that any functionality relies on the logic governing activation of the bypass capability cannot be utilized under TE10.10.01 and TE10.10.02.
AS10.25	TE10.25.02	x	x	x	x		ADDED (No 140-2)	x	x	x		The tester shall verify that the conditional self-tests are performed as specified.
AS10.37	TE10.37.05	x	x	x	x	Software/ Firmware loading	(140-2: TE09.35.05)	x				The tester shall test the module by modifying the software or firmware to be loaded, or the implemented authentication mechanism and initiating the self-test, and observing the output from the status output interface. If no indicator is output that indicates that the software/firmware load test failed, the assertion fails. If it is not possible for the tester to modify the software or firmware to be loaded, or the implemented authentication mechanism, then the vendor shall provide a rationale to the tester why this test cannot be performed.
	TE10.37.06	x	x	x	x	Software/ Firmware loading	ADDED (No 140-2)	x				The tester shall exercise the cryptographic module, with modifying the software or firmware to be loaded, modifying the reference authentication key, or attempting to bypass the implemented authentication mechanism,

												and shall initiate the software/firmware load test. After the self-test fails, the tester shall verify that the loaded software or firmware cannot be used and that the module's versioning information is unchanged.
	TE10.37.09	x	x	x	x	Software/ Firmware loading	ADDED (No 140-2)	x				The tester shall exercise the cryptographic module, without loading the reference authentication key in advance, and shall initiate the software/firmware load test. If the software/firmware load test passes, the assertion fails.
AS10.46	TE10.46.03	x	x	x	x	Manual entry for EDC	(140-2: TE09.40.03)	x				For manual entry tests using an EDC, the tester shall perform the following tests: a. The tester shall enter every manually entered SSP and verify that the procedure used to enter each SSP is in accordance with the documented procedure, including the form that the SSP are in when they are entered. b. The tester shall enter each type of manually entered SSP without any errors and shall verify the status output interface. If no indicator is output, or if the indicator does not match the documented indicator for the success of the manual entry test, the test is failed. c. The tester shall attempt to perform cryptographic operations with each entered SSP to verify that it was entered correctly. d. The tester shall modify either the EDC associated with each manually entered SSP or the SSP itself and shall enter them into the module. The tester shall verify the indicator that is output from the status output interface; if no indicator is output, or the indicator does not match the documented indicator for the failure of the manual entry test, the test is failed. e. The tester shall attempt to perform cryptographic operations with each SSP that was not successfully entered. Each operation using each SSP is required to fail, verifying that the SSP was not entered.
	TE10.46.04	x	x	x	x	Manual entry using duplicate entries of SSP	(140-2: TE09.40.04)	x				For manual entry tests using **duplicate entries of SSPs or key components**, the tester shall perform the following tests: a. The tester shall enter each type of manually-entered SSP without any errors and shall verify the status output interface. If no indicator is output, or if the indicator does not match the documented indicator for the success of the manual entry test, the test is failed. b. The tester shall attempt to perform cryptographic operations with each entered SSP to verify that it was entered correctly. c. The tester shall modify one of the manually entered SSPs, either the first or second duplicate entry, and shall enter them into the module. The tester shall verify the indicator that is output from the status output interface; if no indicator is output, or the indicator does not match the documented indicator for the failure of the manual entry test, the test is failed. d. The tester shall attempt to perform cryptographic operations with each SSP that was not successfully entered. Each operation using each SSP is required to fail, verifying that the SSP was not entered.
AS10.48	TE10.48.03	x	x	x	x	Bypass exclusive	(140-2: TE09.45.03)	x				The tester shall switch the module from the exclusive bypass service to the exclusive cryptographic service and verify that plaintext information is not output.
AS10.49	TE10.49.03	x	x	x	x	Bypass alternate	(140-2: TE09.46.03)	x				The tester shall verify the correct operation of the bypass test by: a. Verifying that the mechanism governing the switching procedure checks to ensure that no alteration of the mechanism has taken place since the last modification. The tester will document the method used. If the design allows, the tester shall modify the mechanism to test the method used. b. modifying the mechanism governing the switching procedure in order to verify the correct operation of the mechanism and to verify the correct operation of the cryptographic service by verifying that the plaintext information is not output.

AS10.53	TE10.53.02	x	x	x	x		(140-2: TE09.12.02)	x	x	x	x	The tester shall initiate the pre-operational self-tests on demand to verify that the initiation of the **pre-operational self-tests** on demand is consistent with the vendor documentation.
	TE10.53.03	x	x	x	x		ADDED (No 140-2)	x	x	x	x	The tester shall initiate the conditional self-tests on demand to verify that the initiation **of the conditional self-tests** on demand is consistent with the vendor documentation.
AS10.54	TE10.54.01			x	x		ADDED (No 140-2)	x	x	x	x	The tester shall verify, by inspection of the cryptographic module, that the pre-operational and conditional self-tests are repeatedly performed as specified in VE10.54.01, and VE10.54.02.
Section 6.11 – Life-Cycle Assurance												
AS11.08	TE11.08.09	x	x	x	x		(140-2: TE04.05.08)	x	x	x	x	The tester shall exercise the cryptographic module, causing it to enter each of its major states. For each state that has a distinct indicator, the tester shall attempt to verify the indicator while the module is in the state. If the expected indicator is not observed, or two or more such indicators are observed at the same time (indicating that the module is in more than one state at one time), this test is failed.
AS11.11	TE11.11.01	x	x	x	x		(140-2: TE04.03.01)	x				From each error state that does not require maintenance, service, or repair, the tester shall verify that the cryptographic module can be caused to transition to an acceptable operational or initialisation state. This effort consists of two parts: first, the tester shall verify that the cryptographic module indicates when it is an error state, and second, that the module operates correctly in this target state. The tester shall report how the requirement was verified (i.e., by code examination or by exercising the module).
AS11.16	TE11.16.01	x	x	x	x	Software/Firmware	ADDED (140-2: TE10.07.01)	x	x	x	x	The tester shall use the list supplied by the vendor to verify that a source listing for each software or firmware component is contained in the module.
AS11.18	TE11.18.01	x	x	x	x	Hardware	ADDED (No 140-2)	x	x	x	x	The tester shall use the list supplied by the vendor to verify that a HDL listing for each hardware component is contained in the module.
AS11.23	TE11.23.01		x	x	x		ADDED (No 140-2)	x	x	x	x	The tester shall verify that the vendor provides documentation that all software or firmware within a cryptographic module is implemented using a high-level, non-proprietary language.
AS11.25	TE11.25.01		x	x	x	Custom integrated circuits	ADDED (140-2: TE10.13.01)	x				The tester shall verify the vendor documentation that the information specified in VE11.25.01 is included.
AS11.32	TE11.32.02	x	x	x	x		(140-2: TE10.03.02)	x	x	x	x	The tester shall perform the procedures for the secure installation, initialisation, and startup of the cryptographic module and verify their correctness.
AS11.38	TE11.38.03	x	x	x	x	For OEUP or PTSC: **Not** required	ADDED (No 140-2)	x (UPDT)			x	The tester shall verify that any CVEs associated with the module: - are not security relevant, or, - if they are security relevant, mitigations provided by the vendor are appropriate.
Section 6.12 - Mitigation of Other Attacks												
	None											
Annex B - Cryptographic Module Security Policy												
	As Required											