**MM Section 7.4 Proposal**

## Remote Testing of Modules

The guidance below addresses the need for testing a module remotely while obtaining the equivalent assurance as if the test were performed at the vendor’s facility. All physical testing which includes hybrid modules **shall** be performed in person by a CSTL tester at either the vendor or the CSTL site.

The CSTL may perform some or all testing remotely. If the testing is performed remotely, the following conditions **shall** be met:

1. a. The hardware, firmware or hybrid IUT is located at the vendor site.

b. The software IUT is located at the vendor site or 3rd party cloud system.

2. The vendor remotely provides a cryptographic module to the test laboratory and its boundary and version are verified against the Security Policy. (TE04.13.01, 02, 03). The module boundary and version **shall** be verified at the beginning of any new remote testing sessions.

3. The network access to a remote test operating environment **shall** be authorized and controlled by the vendor. The cryptographic module under test **shall** be confirmed to be running on an OE that is well-defined and has a specific OS version, hardware platform and version, and processor (including microprocessor version), as shown on the module’s certificate and security policy and where this can be confirmed during the test session. A 3rd party cloud system (e.g., Amazon Web Services, Microsoft Azure, and Google Cloud) may be used if these rules are met and the operating environment provides the same or additional level of security as the lab would provide for internal testing. The tester **shall** have control (oversight) of the testing environment. The tester’s network **shall** be connected to the vendor’s network via a secure connection (e.g., VPN or SSH) as permitted within a signed agreement by the lab and vendor. The tester’s tools must satisfy the lab’s network requirements before connecting to the vendor’s network to test the module.

4. The CSTL **shall** have a procedure for conducting remote testing at the vendor site which includes the following:

a. All the remote testing sessions that produce the final test results **shall** be recorded and archived at the CSTL as evidence material.

b. If multiple remote testing sessions are required, a log which includes the date and the test being conducted **shall** be maintained and archived.

c. If during testing, the IUT version or subversion changes, the final test report being submitted **shall** reflect the final version of the IUT.

d. If there are multiple simultaneously testing activities occurring at the vendor site, a system of separation between the different product test activities **shall** be maintained.

e. For all conformance testing and validations, the CSTL **shall** ensure that any file containing iterative, not final, test results are isolated from the final test results

f. It is the CSTL’s responsibility to ensure that any version iteration during the testing doesn’t impact any of the final results transmitted to the CMVP.

5. The required operating environment information (e.g., operating system name and version, processor family, hardware platform model) **shall** be obtained and verified against the operating environment information listed on the CAVP algorithm certificates for this module.

6. The tester **shall** understand, direct, and assume control of testing operations to initialize, install, and operate the module.

7. If a test harness is used, it **shall** be reviewed or written by the lab. It **shall** be verified to have been maintained properly with no vendor manipulation prior to its execution. The test results on the remote operating environment **shall** be captured and transmitted back to lab without the risk of being modified. The tester **shall** verify the test harness runs properly on its operating environment. The tester must verify the integrity of the testing session as well as the completeness and accuracy of the test results.

8. The vendor may provide assistance, under the direction of the tester, to obtain evidence of test results or restarting the operating environment as a means to recover from the induced error state of the cryptographic module.

9.The remote testing **shall** cover the same set of FIPS 140-3 requirements including but not limited to the following list, as if the operating environment were local to the tester:

a. The services listed in the module Security Policy can be invoked and verified by the tester.

b. For a module to be validated at Level 2 or 3 for ISO/IEC 19790:2012 Section 7.4.4, the role-based or identity-based authentication **shall** be performed and verified by the tester.

c. The failure of self-tests and the subsequent transition to an error state where module data output interfaces are inhibited can be observed and verified by the tester.

e. As applicable per IG 9.3.A, entropy has been effectively analyzed and received an ESV for all specific OEs and/or platforms prior to submission.

10. The test report **shall** document how the above conditions are met.

The vendor must provide a signed affirmation letter to the lab describing the remote testing process and access control mechanism that allows the lab to perform the test on the remote operating environment and protects the integrity of the test results. The lab **shall** provide a signed letter to the CMVP stating that the module had been tested remotely, affirming that the vendor provided their affirmation letter, stating what TEs were tested remotely, and explaining how the requirements were met during the remote testing.

It is the CSTL’s responsibility to ensure that the assurance level is maintained when remote testing is being conducted.

Additional Comments:

1. It is the responsibility of the tester to determine if a module is eligible to be tested remotely. If the tester cannot confirm a test requirement during remote testing, then the module **shall** not be fully tested remotely. If the tester wishes to test a subset of test requirements remotely, the remaining test requirements **shall** be tested onsite.

2. The tester **shall** confirm that the operating environment exactly matches the agreed upon test environment, including any virtual environments used. A Virtual Machine may not be used in lieu of an OS, unless the VM has been agreed to be part of the test environment and will be listed on the certificate.

3. A record of the testing location and CSTL tester(s) who conducted the testing **shall** be maintained. This is applicable for all tests including physical testing.

4. Regardless of the location of the testing, it is the CSTL’s responsibility to ensure that all HB 150 requirements are met including tools requirements for physical testing.