

**INFORMATION TECHNOLOGY SECURITY TESTING
TEST METHOD SELECTION LIST - COMMON CRITERIA TESTING**

Instructions: Check 26/A01 and each test method for which you are requesting accreditation. Minimum test methods required for 26/A01 accreditation are APE, ASE, and EAL1.

COMMON CRITERIA TESTING (CCT)

<i>NVLAP Test Method Code</i>	<i>Test Method Designation</i>
_____ 26/A01	ISO/IEC 15408: Information Technology—Security Techniques—Evaluation Criteria for IT Security Common Evaluation Methodology for Information Technology Security, Part 1 - Introduction and general model Common Methodology for Information Technology Security Evaluation, Part 2 - Evaluation methodology
_____	26/A01a APE: Protection Profile evaluation
_____	26/A01b ASE: Security Target evaluation
_____	26/A01c EAL1: Evaluation assurance level 1
_____	26/A01d EAL2: Evaluation assurance level 2
_____	26/A01e EAL3: Evaluation assurance level 3
_____	26/A01f EAL4: Evaluation assurance level 4

Complete the Application Supplement on back of this page.

INFORMATION TECHNOLOGY SECURITY TESTING APPLICATION SUPPLEMENT - COMMON CRITERIA TESTING

QUALITY MANUAL (see NIST Handbook 150:2001, subclause 4.2)

Please provide NVLAP with a copy of your laboratory quality manual with your initial application and with each annual renewal application. The manual may accompany this application or may be sent at a later date, however, NVLAP will take no action on your application until the manual is received. The NVLAP on-site assessor(s) will review the manual before conducting the on-site assessment of your laboratory, will review it with you during the on-site, and will return it to you afterwards.

PROFICIENCY TESTING (see NIST Handbook 150:2001, subclause 3.3)

All laboratories must participate in proficiency testing for this LAP. Upon a positive review of the quality manual, NVLAP will send to you the necessary materials for conduct of the proficiency testing. It is estimated that the proficiency testing for initial accreditation will require three people a period of two weeks to complete.

NVLAP will evaluate the test results submitted by your laboratory and the results will be reviewed with you during the on-site assessment. If the test results submitted are not satisfactory, the results will be discussed with you and additional time will be given for further work.

Proficiency testing will be conducted before initial accreditation and may be required every other year thereafter—in the year when there is no on-site assessment. The time required to complete proficiency testing after the initial round is planned to be less than for the initial round.

ON-SITE ASSESSMENT (see NIST Handbook 150:2001, subclause 3.2)

After a successful review of the quality manual and successful completion of proficiency testing, the on-site assessment will be scheduled. The assessment team will consist of two or three people. The visit will be for two full days and the morning of the third day.

INFORMATION TECHNOLOGY SECURITY TESTING TEST METHOD SELECTION LIST - CRYPTOGRAPHIC MODULE TESTING

Instructions: For FIPS 140-2, check 17/C03 and each Test Method Group for which you are requesting accreditations. Group 1 is required; Group 4 and Group 5 are optional. For FIPS 140-1, check 17/C01 and each Test Method Group for which you are requesting accreditations. Group 1 is required; Group 2 and Group 3 are optional.

For acceptance by the NIST/ITL and CSE Cryptographic Module Validation Program, a laboratory must be accredited for both 17/C03 and 17/C04. If the laboratory is going to offer services for FIPS 140-1, then both 17/C01 and 17/C02 are also required.

CRYPTOGRAPHIC MODULE TESTING (CMT)

<i>NVLAP Test Method Code</i>	<i>Test Method Designation</i>
_____ 17/C01	NIST-CSTT:140-1; National Institute of Standards and Technology - Cryptographic Support Test Tool (CSTT) for the Federal Information Processing Standard 140-1 (FIPS 140-1), "Security Requirements for Cryptographic Modules."
_____ 17/C01a	Test Method Group 1: All test methods in accordance with FIPS 140-1 and specified in the CSTT, except those listed in Group 2 and Group 3.
_____ 17/C01b	Test Method Group 2: Test methods for Physical Security, Level 4 in accordance with FIPS 140-1 and specified in the CSTT.
_____ 17/C01c	Test Method Group 3: Test methods for Software Security, Level 4 in accordance with FIPS 140-1 and specified in the CSTT.
_____ 17/C02	FIPS-Approved and NIST-recommended Cryptographic Algorithms (see http://csrc.nist.gov/cryptval) as required in FIPS PUB 140-1.
_____ 17/C03	NIST-CSTT:140-3; National Institute of Standards and Technology - Cryptographic Support Test Tool (CSTT) CRYPTIK for the Federal Information Processing Standard 140-2 (FIPS 140-2), "Security Requirements for Cryptographic Modules."
_____ 17/C03a	Test Method Group 1: All test methods in accordance with FIPS 140-2 and specified in the CSTT, except those listed in Group 4 and Group 5.
_____ 17/C03b	Test Method Group 4: Test methods for Physical Security, Level 4 in accordance with FIPS 140-2 and specified in the CSTT.
_____ 17/C03c	Test Method Group 5: Test methods for Software Security, Level 4 in accordance with FIPS 140-2 and specified in the CSTT.
_____ 17/C04	FIPS-Approved and NIST-recommended Cryptographic Algorithms (see http://csrc.nist.gov/cryptval) as required in FIPS PUB 140-2.

Complete the Application Supplement on back of this page.

INFORMATION TECHNOLOGY SECURITY TESTING APPLICATION SUPPLEMENT - CRYPTOGRAPHIC MODULE TESTING

QUALITY ASSURANCE MANUAL (see NIST Handbook 150:2001, subclause 4.2)

Before your initial on-site and for renewals requiring an on-site assessment, please provide NVLAP with a copy of your laboratory quality manual and test procedures, including specifics for CMT testing. The manual and procedures may accompany this application or may be sent at a later date. The NVLAP on-site assessor(s) will review the manual *before conducting* the on-site assessment of your laboratory and return it afterwards.

PROFICIENCY TESTING (see NIST Handbook 150:2001, subclause 3.3)

Proficiency test demonstrations are required during on-site assessments and periodically thereafter. Laboratories will be notified concerning the required proficiency testing schedules and activities.

During the initial on-site assessment, a demonstration of testing capability of a cryptographic artifact will be required. A specially designed artifact will be provided by the assessor(s).

ON-SITE ASSESSMENT (see NIST Handbook 150:2001, subclause 3.2)

The typical on-site assessment for FIPS 140-2 is two days in length. Assessment for 17/C01 and 17/C02 (FIPS 140-1) does not require additional assessment days.