DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
National Voluntary Laboratory Accreditation Program

ISSUE DATE:
January 31, 2017

LAB BULLETIN

NUMBER: LB-99-2017

LAP: Cryptographic and Security Testing

SUBJECT: Administration of the CMVP Exam Transitioning to Pearson VUE

Expected during the third quarter of calendar year 2017 the administration of the CMVP remote proficiency/round-table quiz (Ref: NVLAP LB-87-2015) will transition from the Cryptographic Module Validation Program staff to Pearson VUE, an independent computer-based-testing company. The quiz will be an individual certification exam.

Laboratories that are currently scheduling remote quizzes and on-site assessments will complete the assessments using the current process. Laboratories that have already completed the assessments using the current process will transition to the updated process during the next assessment cycle.

The certification exam will encompass the same domains as listed in NIST Handbook 150-17, Annex B; however, the grouping will be modified. (See Appendix A of this bulletin.) The certification exam will be pass/fail, closed-book, and computer-based with 100 multiple choice questions. The amount of time to complete the certification exam has not been finalized, but it is expected to be less than six hours.

Laboratories will be required to have a minimum of two Cryptographic Validation Program (CVP) FIPS 140 Certified Testers throughout the accreditation period. Laboratories will continue to be required to notify NVLAP and CMVP of any personnel changes within thirty (30) days. Failure to communicate laboratory changes to NVLAP and CMVP may result in an adverse action regarding accreditation.

Passing the certification exam is the only requirement for becoming a CVP Certified Tester. CMVP will receive a copy of all exam results and maintain a list of CVP Certified Testers. Maintaining the certification will require individuals to periodically retake and pass the certification exam. However, those details have not been finalized.

Because the certification exam will be administered to individuals, the certification lies with the individuals and not the employer. Only individuals authorized by CMVP will be permitted to schedule the exam with Pearson VUE. The specific process for requesting authorization is still being defined but it is expected that a point of contact at each laboratory will be asked to nominate those testers to CMVP.

Approved signatories and independent testers will be required to pass the certification exam to continue in their roles. (Independent testers are those who perform testing with little or no oversight.) Testers who do not take or pass the exam (e.g. testers in training) will be required to have oversight from testers who have passed the exam. Individuals will be able to schedule the exam directly with Pearson VUE up to 24 hours prior to the start of the exam. Individuals will also be able to cancel or reschedule their exam directly with Pearson VUE.

The certification exam is graded immediately allowing the tester to know his/her pass/fail status before departing. Pearson VUE has testing locations throughout the world. All laboratories have at least one testing center within 30 miles of their laboratory location.

The cost for each individual to take the certification exam is still being negotiated. The certification exam fee is expected to be paid by the individual or the laboratory (on behalf of the individual) directly to Pearson VUE. The fee is not associated with NVLAP and will not be collected by NVLAP.

Questions regarding the changes to the NVLAP CST LAP requirements should be directed to Brad Moore, brad.moore@nist.gov, 301-975-5740.

Appendix A

Domain 1: Physical Security (10%)

- Understand the different embodiments for modules
- Understand requirements for physical security for modules specific to levels 1-3
- Understand the requirements for physical security for modules specific to level 4

Domain 2: Authentication, Roles, Services, and Operational Environment (16%)

- Understand authentication requirements and concepts
- Define the requirements for role
- Understand the concepts of services using approved and non-approved functions, and bypass
- Understand the concepts of reviewing and testing Software Modules
- Describe the operational environment requirements/concepts and how to test them

Domain 3: Algorithms & Self-Tests (24%)

- Understand the concepts of the approved and allowed algorithms
- Identify which algorithms are approved or allowed
- Understand the issues related to testing the components of the algorithms
- Identify the tester's responsibilities when reviewing an algorithm's implementation
- Identify the power-up tests and know the associated requirements
- Understand the requirements for conditional tests

Domain 4: Key Establishment (24%)

- Understand the requirements for key generation, key agreement, key transport and key derivation and applicable standards and guidance
- Understand and identify the approved random bit generators
- Understand the notion of entropy and methods of entropy estimation
- Possess general knowledge of the key establishment protocols and standards in the IT industry

Domain 5: Key Management (11%)

- Understand the requirements for key entry/output and trusted paths
- Understand the requirements for key storage
- Understand the various types of key and CSP zeroization

Domain 6: Security Assurances (15%)

- Understand the requirements of module specification including approved and non-approved modes
- Understand the FIPS Standards, programmatic guidance, implementation guidance and associated documentation requirements

- Understand the requirements for ports & interfaces, finite state model, EMI/EMC, Mitigation of Other Attacks and design assurance
- Understand the concept and testing requirements for formal modeling