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

LAB BULLETIN

ISSUE DATE:
November 23, 2016

NUMBER: LB-96-2016

LAP: Cryptographic and Security Testing

SUBJECT: HB 150-17, Annex B - Testing Conducted at Permanent Remote Locations

Overview

NIST Handbook 150 requires a description of the laboratory be provided as it applies to NVLAP accreditation activities. An on-site laboratory assessment is a systematic, independent, documented process for determining laboratory competence and for reviewing records, statements of fact or other relevant information by NVLAP assessors at the laboratory facilities and other places where test or calibration services are provided with the objective of determining the extent to which NVLAP requirements are fulfilled. A laboratory's activities may be carried out at a permanent, temporary, or remote location. NVLAP further defines a laboratory as being a physical entity—that is, a testing or calibration facility that is separate and apart physically from any other laboratory whether or not sharing common ownership, management, or quality systems with any other laboratory(s). The management system shall cover testing carried out at the laboratory's permanent facilities and at sites away from its permanent facilities, or in associated temporary, mobile, or remote facilities.

NIST Handbook 150-17 further states in Clause 5.3.6: If a laboratory must conduct conformance testing at a location outside the laboratory facility, the environment shall conform, as appropriate, to the requirements for the laboratory site, and shall be checked by the NVLAP-accredited laboratory as a responsible party for the security of the environment and the integrity of all tests and recorded results.

The requirements set out in this bulletin apply only to permanent remote locations (e.g. work-at-home, small remote offices), known hereafter as remote locations.

- Temporary off-site locations may be used for performing physical testing (e.g. vendor sites or specialized physical testing facility such as a university lab).

- Mobile facilities are not approved for any cryptographic and security testing activities.

Requirements for testing at permanent remote locations

A NVLAP CST accredited laboratory may perform IUT testing at laboratory remote locations without a remote location site visit by NVLAP assessors with the following conditions:

1. The laboratory shall have a procedure for the protection of all IUT information. The procedure shall address, but not be limited to:

    a. VPN connections which may be used to transmit IUT information between laboratory locations;

    b. Workstations, laptops, and storage devices (e.g. memory sticks, hard drives, etc.);

    c. Authenticated access to workstations, laptops, etc. by lab personnel only;

d. Protection of data (source code, HDL, documentation, etc.). Access, use, storage, and destruction shall be defined and documented for both electronic and physical documents.

2. All workstations or test equipment shall be supplied by and under the control of the laboratory. Programmatic tools shall only be installed on laboratory owned equipment.

3. Hardware IUTs shall not be present at a remote location.

4. Software or firmware IUT operating environment platforms shall not be present at remote locations. Software or firmware IUT operational testing may be performed from a remote location utilizing a VPN connection to the operating environment platform(s) located at the permanent laboratory facility.

5. Documentation review and code review are permitted at remote locations.

6. The laboratory shall disclose to the IUT vendor that the vendor's IUT information may be maintained at remote locations.

7. The laboratory shall establish and maintain procedures for record management (ref. NIST HB 150, sec. 4.13.1) at remote locations. Regardless, a copy of all management system and technical records shall be retained at the laboratory's permanent location.

8. The quality manual shall state what work may be performed at any remote locations. (e.g. CAVS, document review, source code review, CRYPTIK entry, etc.).

9. The laboratory's internal audit schedule and procedure shall also include remote locations.

10. The test records for each project shall define the work performed at each laboratory location, if applicable. (e.g. CAVS, document review, source code review, CRYPTIK entry, etc.).

Questions should be directed to Brad Moore, brad.moore@nist.gov, 301-975-5740.