Validation Scope for Entropy Sources
17ESV

SP 800-90B Entropy Source Validation Workshop

Thursday April 29, 2021

Brad Moore (NVLAP)
Chris Celi (NIST)

National Voluntary Laboratory Accreditation Program
National Institute of Standards and Technology
Gaithersburg, Maryland

NVLAP

Accreditation Body

authoritative body that performs accreditation

[ISO 17000:2020 Conformity assessment – Vocabulary and general principles, 4.7]

Accreditation

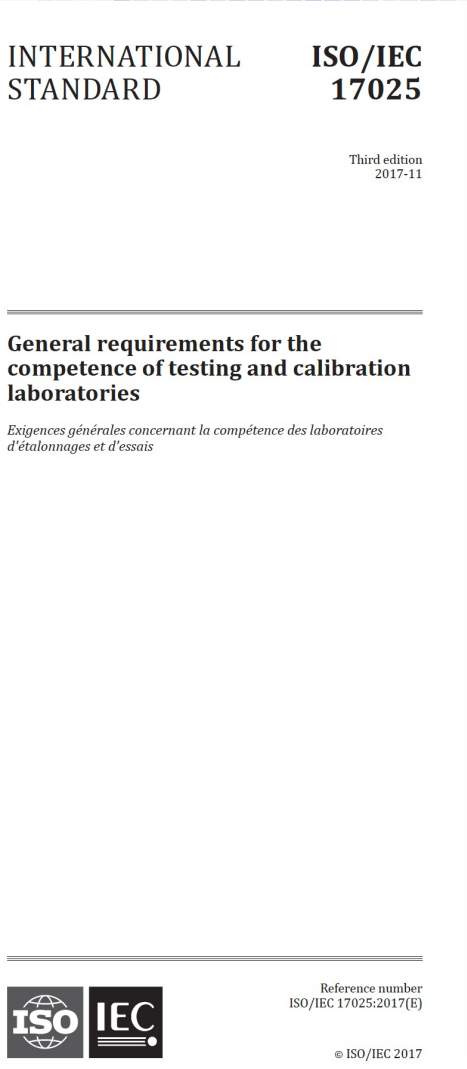
- third-party *attestation* related to a *conformity assessment body*, conveying formal demonstration of its competence, *impartiality* and consistent operation in performing specific conformity assessment activities

[ISO 17000:2020 Conformity assessment – Vocabulary and general principles, 7.7]

NVLAP Operations

All NVLAP accreditation programs in accordance with ISO/IEC 17025 – *General require for the competence of testing anc calibration laboratories.*

The NVLAP accreditation program voluntary and available to any lab meeting the application requirem a specific program.


INTERNATIONAL STANDARD

ISO/IEC 17025

Third edition
2017-11

General requirements for the competence of testing and calibration laboratories

Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais

ISO IEC

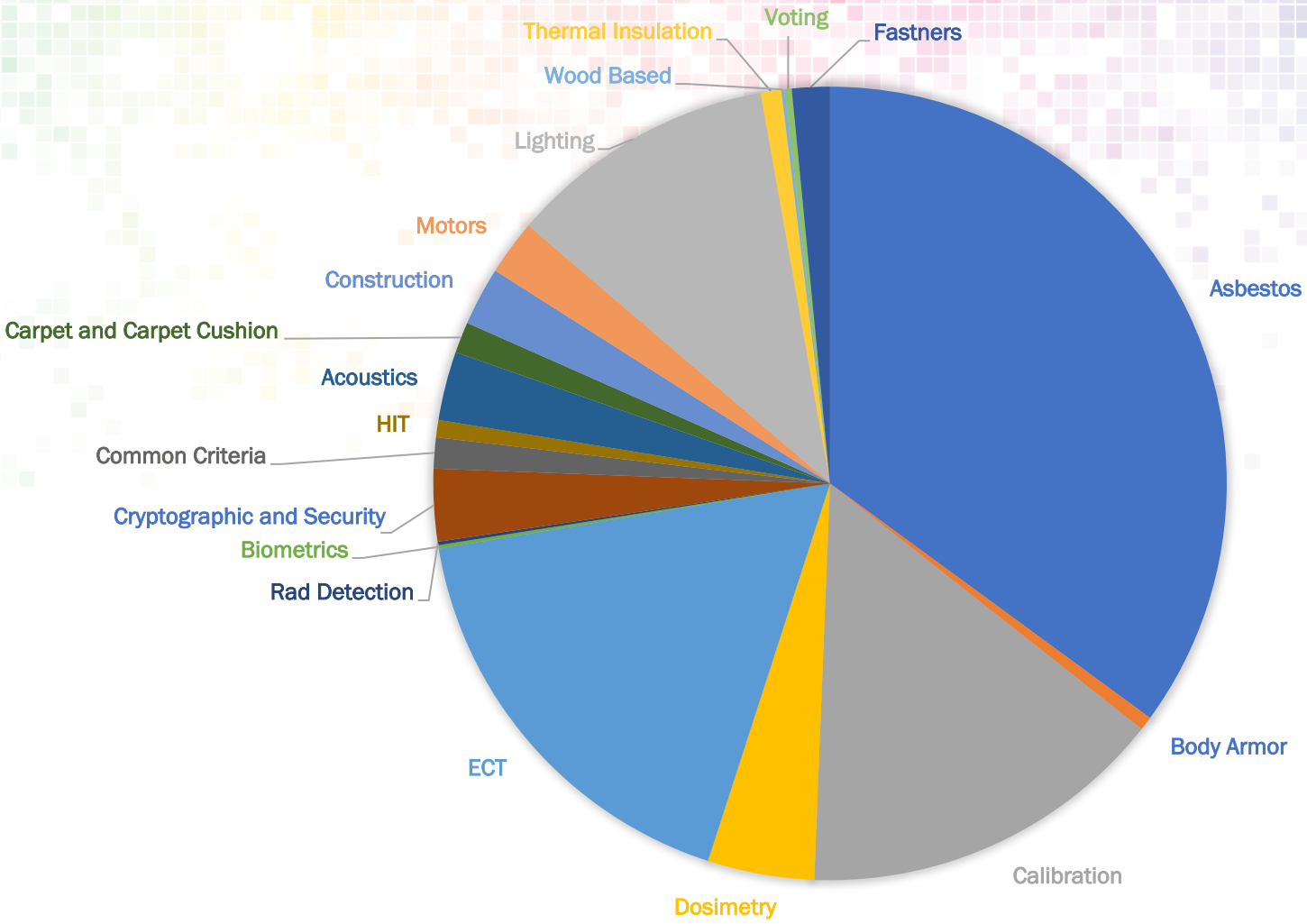
Reference number
ISO/IEC 17025:2017(E)

© ISO/IEC 2017

Mutual Recognition Arrangements

- ILAC - International Laboratory Accreditation Cooperation (Full Member)
  - ILAC MRA Text (ILAC P5:06/2017) (PDF)
  - ILAC Membership
  - ILAC Newsletter
- APAC - Asia Pacific Accreditation Cooperation (Full Member)
  - APLAC MRA Text
  - APLAC Membership
  - APLAC News
- IAAC - Inter American Accreditation Cooperation (Full Member)
  - IAAC MLA Text (PDF)
  - IAAC Membership
  - IAAC News

NVLAP Accreditation Programs



Cryptographic and Security Testing LAP

- The Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP), initially named Cryptographic Module Testing (CMT), was established by NVLAP to accredit laboratories that perform cryptographic modules validation conformance testing under the Cryptographic Module Validation Program (CMVP).

- *NIST HB 150-17:2020; Cryptographic and Security Testing* Program Specific Requirements
  - *Annex B* – Cryptographic Algorithms and Cryptographic Modules Testing
  - *Annex C* – Personal Identity Verification (PIV)
  - *Annex D* - General Services Administration Precursor (GSAP)
  - *Annex E* – Security Content Automation Protocol Testing (SCAP)
  - Annex F - DHS Identity and Privilege Credential Management Testing (TWIC ®)
  - *Annex G* – Automated Cryptographic Validation Testing (ACVT)
  - ***Annex H Entropy Source Validation (ESV)***

CST LAP – Accreditation Requirements

- ISO/IEC 17025:2017, *General Requirements for the Competence of Testing and Calibration Laboratories.*

- NIST HB 150:2020, *NVLAP Procedures and General Requirements*

- NIST HB 150-17:2020; NVLAP Cryptographic and Security Testing
  - *Currently under revision – for FIPS 140-3 and other general updates*
  - *A second revision – to include the new Annex "H" - ESV accreditation requirements* [expected FY22 - Q2]

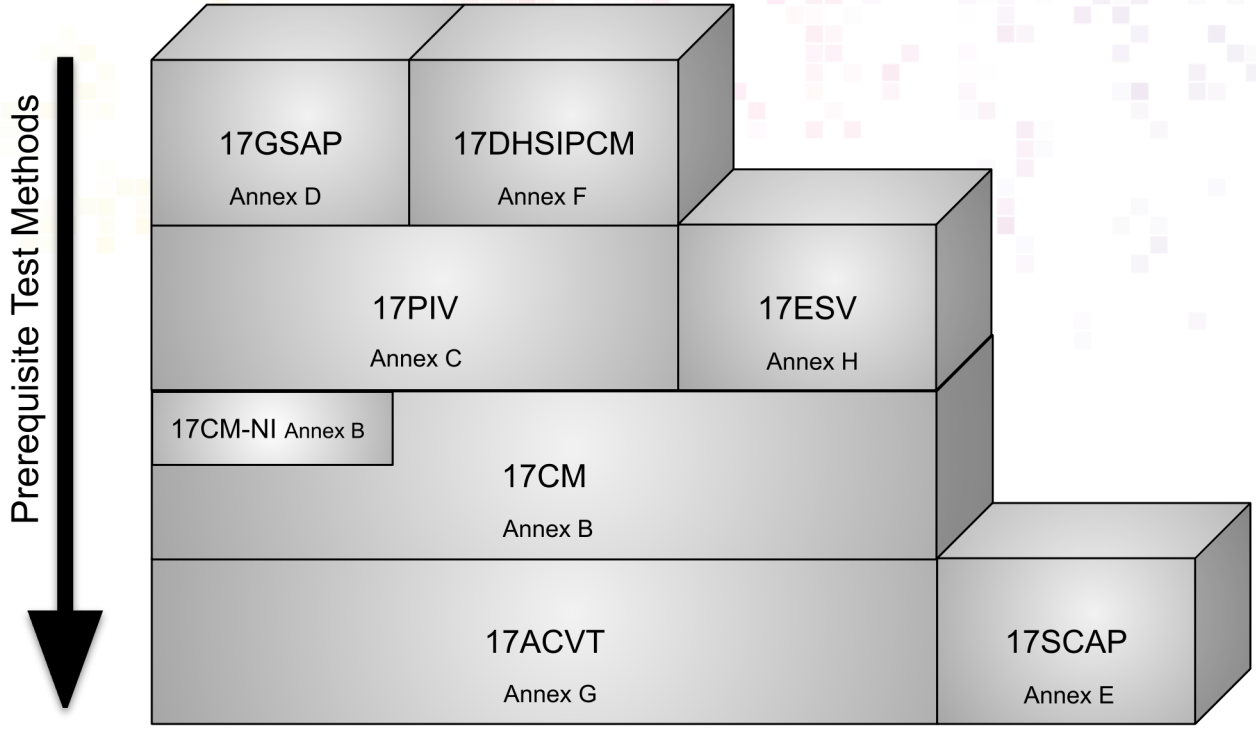
Entropy Source Validation Scope (HB 150-17, Annex H)

- Conformance Testing (from SP 800-90B)
  - Conformance testing for implementations of this Recommendation will be conducted within the framework of the Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP). The requirements of this Recommendation are indicated by the word "**shall.**" Some of these requirements may be out-of-scope for CAVP or CMVP validation testing, and thus are the responsibility of entities using, implementing, installing or configuring applications that incorporate this Recommendation.

Entropy Source Validation Scope (HB 150-17, Annex H) Requirements

- Optional additional scope
- Lab must already be accredited under 17CM and 17ACVT
- Third-party labs
- Two Subject Matter Experts (SMEs)
  - Accreditation exam, similar to 17CM
    - May be different SMEs than the 17CM CVP Certified Testers
  - Responsible for data collection and report submission
  - Will be given access to ESVTS Prod environment after accreditation is met

HB 150-17 Annexes



HB150-17 Timelines

- 17ESV (HB 150-17, Annex H) - expected FY22, Q2
- Existing 17CM third-party labs, will be recognized by the CMVP for 17ESV **but must still go through the NVLAP scope expansion process by a later specified date**
  - Failure to meet the accreditation requirements by the specified date will lead to revocation of existing validations
  - Expectation is 1 year after HB 150-17 publication
  - Production access must still be requested

Entropy – Accreditation Scope Expansion

Lab Submission Package:

1) Lab's internal ***SP*** **800-90B** *(ESV) testing procedures;*

2) Staff training / qualification for ***NIST SP 800-90B (ESV);***

3) A lab-submitted and self-assessed NIST HB 150-17, Annex H checklist [In development].

4) Additional technical record requirements [in development]

Questions

- Brad Moore
- Accreditation Program Manager
- bradley.moore@nist.gov
- https://www.nist.gov/nvlap

- Chris Celi
- CAVP Program Manager
- christopher.celi@nist.gov