

|                                                                                          |                                                                                                                                        |                                                                                        |
|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
|         | <b>DEPARTMENT OF COMMERCE</b><br>National Institute of Standards and Technology<br>National Voluntary Laboratory Accreditation Program | <b>ISSUE DATE:</b><br>October 20, 2026                                                 |
|                                                                                          | <b>LAB Bulletin</b>                                                                                                                    | <b>NUMBER:</b><br>LB-167-2026<br><br><b>LAP:</b><br>Cryptographic and Security Testing |
| <b>SUBJECT:</b> Update to Entropy Source Validation test standard and submission process |                                                                                                                                        |                                                                                        |

The purpose of this bulletin is to notify all laboratories currently accredited in the Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP) of an update in the Entropy Source Validation (ESV) test standard and submission process and edits to the relevant clauses in Handbook 150-17, Annex H.

## Background

On May 7, 2026, the Cryptographic Module Validation Program (CMVP) opened a new submission process for SP 800-90C Random Bit Generator Constructions for validation. This standard builds upon SP 800-90B on Entropy Sources that is used as the basis for Entropy Source Validation (ESV) testing. The augmented validation track is now available to laboratories to upgrade their accreditation for ESV testing.

## Notice

Effective immediately, the following update applies to Handbook 150-17:2022 Annex H.1:

In addition to validating cryptographic modules, the CMVP also validates entropy sources and random bit generator constructions that may be integrated in one or more cryptographic modules. The program provides Federal agencies—in the United States and Canada—confidence that a properly configured, validated entropy source and random bit generator will provide sufficient randomness for cryptographic operations.

Entropy sources and random bit generators may be validated with or without an underlying module. This is done through the CMVP and the Entropy Source Validation Testing System (ESVTS). ESVTS includes automated testing as defined in SP 800-90B and SP 800-90C and manual review of justifications of conformance to other non-testable SP 800-90B and SP 800-90C requirements. The ESV testing may only be accredited to third-party testing laboratories.

Laboratories accredited for ESV testing report the statement of conformance of entropy sources and random bit generators to the recommendations in the applicable versions of FIPS 140 Annexes (and all superseded versions). The CMVP holds the role of validation authority and awards validation certificates for implementations that successfully satisfy the program’s validation requirements. Laboratories accredited under this scope must leverage the ESVTS service as their “means of testing” to maintain accreditation.

Any future ESV assessments will be subject to the requirements introduced in this lab bulletin. During this assessment, the laboratory will be expected to demonstrate the submission of an entropy source and a random bit generator to the CMVP, address SP 800-90B and SP 800-90C requirements during the subject matter expert proficiency exam and demonstrate how the laboratory meets the requirements of the annex with regards to entropy source submissions and random bit generator submissions (such as retrieving validation records). These new expectations are in addition to the previous expectations, not replacing them.

Based on the updated ESV test and submission process, NVLAP has updated its CST LAP to incorporate these updates by revising laboratory accreditation scopes to reflect current capability as follows:

### **Entropy Source Validation Testing System (ESVTS)**

| <b><u>Code</u></b> | <b><u>Description</u></b>                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 17/ESV01           | Entropy Source Validation Testing (ESVT) as defined in SP 800-90B requirements for all FIPS-approved entropy sources as required in applicable versions of FIPS 140 Annexes (and all superseded versions) |

Laboratories accredited for ESV testing will receive a revised scope reflecting this updated verbiage.

For laboratories currently accredited for ESV testing in the NVLAP CST program, self-declaration to compliance with testing requirements must be submitted in writing (an e-mail request is sufficient) to request the update to the scope of accreditation. With the written request, each applicant must also provide:

- The NVLAP CST LAP Self-Declaration of Implementation form (October 2026 version), for CST ESV accreditation updates, signed by the laboratory's authorized representative, with applicable supporting documentation; and
- A current list of subject matter experts proficient for SP 800-90C.

Once this information is received, NVLAP will proceed with a documentary review. If this information is determined to be incomplete, follow-up information will be requested. The testing will be assessed during the laboratory's next onsite assessment.

Once the attestation and review process are successfully completed, the laboratory's scope will be updated to reflect ESV testing capability as follows:

| <b><u>Code</u></b> | <b><u>Description</u></b>                                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 17/ESV02           | Entropy Source Validation Testing (ESVT) as defined in SP 800-90B and SP 800-90C requirements for all FIPS-approved entropy sources and random bit generators as required in applicable versions of FIPS 140 Annexes (and all superseded versions) |

Any laboratory that has not submitted the attestation and documents or undergone an ESV assessment by December 1, 2026, will not be permitted to submit reports for validation for SP 800-90C.

Questions should be directed to the NVLAP program manager, Janneth Marcelo at [janneth.marcelo@nist.gov](mailto:janneth.marcelo@nist.gov).