## For module submitters:

* How will a module reference an “E” (validated) or “EID” (in progress) ESV entropy source:
  + **On the module certificate**:
    - For FIPS 140-2:
      * For an entropy source that is already validated, the “E” would be on the approved line of the certificate (similar to other approved algorithms). Specifically, “ESV (Cert. #E123)”.
      * If the entropy source is still in progress, the “EID” would need to be completed before the lab can submit the module report to the CMVP.
      * The CMVP will not accept a submission with no ESV certificate, if applicable.
      * An entropy caveat may apply per IG 7.14.
    - For FIPS 140-3:
      * Enter the ESV certificate number within the appropriate field in WebCryptik. It will automatically generate the entry on the module certificate based on this information.
      * If the entropy source is still in progress, the “EID” would need to be completed before the lab can submit the module report to the CMVP.
      * The CMVP will not accept a submission with no ESV certificate, if applicable.
      * An entropy caveat may apply per IG 9.3.A.
  + **In the module Security Policy**:
    - For FIPS 140-2:
      * Use the module certificate terminology above for documenting entropy sources in the Approved Algorithm table of the SP.
      * Indicate how the module is compliant to the ESV entropy source public use document, including a reference link. For example, the configuration and other steps necessary to operate the entropy source in a compliant manner.
      * Per IG 7.18, document the overall amount of generated entropy and the estimated amount of entropy per the source’s output bit.
      * Documentation as required by IG 7.14 (including the porting guidance, if applicable).
      * If applicable per IG 7.20, further explain the nature of the module’s entropy sources, specify which of them are creditable, and indicate if Method 1 or Method 2 is used for entropy calculation.
      * If the module supports a CTR\_DRBG without a derivation function, the seed must supply full entropy, per SP 800-90A, IG D.L. The submitter should check the entropy claim and verify full entropy is supported.
    - For FIPS 140-3 (use the following instructions until superseding guidance is present in SP 800-140Brev1):
      * Use the module certificate terminology above for documenting entropy sources in the Non-Deterministic Random Number Generation Specification table from SP 800-140B. Per IG D.J, document the overall amount of generated entropy and the estimated amount of entropy per the source’s output bit.
      * In Section B.2.9 Sensitive security parameters management, indicate how the module is compliant to the ESV entropy source public use document, including a reference link. For example, the configuration and other steps necessary to operate the entropy source in a compliant manner.
      * Documentation as required by IG 9.3.A (including the porting guidance, if applicable).
      * If applicable per IG D.O, further explain the nature of the module’s entropy sources, specify which of them are creditable, and indicate if Method 1 or Method 2 is used for entropy calculation.
      * If the module supports a CTR\_DRBG without a derivation function, the seed must supply full entropy, per SP 800-90A, IG D.L. The submitter should check the entropy claim and verify full entropy is supported.
  + **In the Test Report**:
    - For FIPS 140-2, apply the below AS/TE’s as they relate to the ESV, in addition to what is already required by the AS/TE’s.
      * TE.01.12.01 - Use the module certificate terminology above for documenting entropy source(s).
      * TE.07.03.01 – Indicate the keys & CSPs: DRBG Internal State, DRBG entropy input, Keys and bits of entropy values
      * TE.07.08.01 – Indicate approved RNGs.
      * TE.07.10.01 – Vendor document specifies all RNGs - RNG & Primary source of entropy
      * AS.07.13 - Include which scenario of IG 7.14 the module is compliant to. Include rational of whether an entropy caveat is applicable per IG 7.14 as it relates to the entropy/DRBG strengths and maximum key sizes generated.
      * AS.07.15 – Determine if intermediate values are output and if so how they meet this assertion.
      * TE.09.04.03 – Verification that each error state entered (including those from ESV failures) are the same as specified in the documentation.
      * TE.09.07.01 Documentation requiring a list of self-tests, including the ESV self-tests.
      * TE.09.07.02 Error condition name, including any specific to the failure of the ESV.
      * TE.09.07.03 Cause an error condition and attempt to clear the error.
      * TE.09.09.01 Documentation requiring the running of self-tests.
      * TE.09.09.02 Verification that the module performs the power-up self-tests.
      * TE.09.10.01 Documentation that shows the indicator that the module outputs on successful completion of power-up self-tests.
      * TE.09.10.02 Verification that the module outputs on successful completion of power-up self-tests an indicator.
    - For FIPS 140-3, apply the below AS/TE’s as they relate to the ESV, in addition to what is already required by the AS/TE’s.
      * TE02.20.01 - Use the module certificate terminology above for documenting entropy source(s).
      * AS09.04 – Confirm RBG state information and intermediate key generation values are considered CSPs.
      * TE09.05.01 – Indicate the keys & CSPs: DRBG Internal State, DRBG entropy input, Keys and bits of entropy values.
      * AS09.06 – Indicate approved RBGs (both DRBGs and entropy sources) and how they are used for the approved security function, SSP generation and/or SSP establishment methods.
      * AS09.08 - Include which scenario of IG 9.3.A the module is compliant to. Include rational of whether an entropy caveat is applicable per IG 9.3.A as it relates to the entropy/DRBG strengths and maximum key sizes generated.
      * AS10.07 – Self-tests (power-on and conditional), error condition(s), self-tests in approved / non-approved modes and without operator intervention.
      * AS10.08 – Error states and indicators.
      * AS10.10 – Cannot utilise functionality that relies upon a function or algorithm that failed a self-test until the self-test passes.
* Note, the above list is not exhaustive of entropy information that needs to be included in a CMVP submission but highlights the key areas to pay attention to in relation to referencing the validated entropy source.