8.4.3 Entry of Entropy Input into a DRBG Boundary

8.4.3.1 Introduction

The bits containing entropy (the entropy input) **shall** be entered into the DRBG boundary either manually, electronically or obtained from within a cryptographic boundary containing the DRBG boundary (see Section 8.2).

Entropy input within a DRBG boundary **shall never** leave the DRBG boundary.

Documentation **shall** specify the intended methods for the entry of entropy input. Documetation **shall** also specify the procedures to be employed to provide entropy input to the DRBG.

8.4.3.2 Manual Entry

When entered manually, the entropy input is entered through the FIPS 140-2 cryptographic boundary into the DRBG boundary (see Section 8.2).
For security levels 1 and 2 FIPS 140-2 cryptographic modules:

- The entropy input may be entered in plaintext form. Alternatively, the entropy input may be entered in encrypted form or in the form of components; in this case, refer to the discussion below for security levels 3 and 4.
- When entered in plaintext form, the same input **shall** be either entered twice or an error detection code (EDC) of at 16 bits **shall** be used to ensure correct entry. Dual control procedures **shall** be used to assure the security of the entry process.
- Entropy input that enters the cryptographic boundary **shall** move directly into the DRBG boundary without being stored, combined or otherwise processed by processes outside the DRBG boundary.
  - Verification of the correct entry of the entropy input (i.e., comparing duplicate entries or verifying the EDC) **shall** be performed only within the DRBG boundary.
  - Other processes within the DRBG boundary **shall not** store, combine or otherwise process the entropy input.
  - After entry verification, the entropy input **shall only** be used to generate seed material.

For security level 3 and 4 FIPS 140-2 cryptographic modules:

- The entropy input **shall** be entered into the cryptographic module in either encrypted or entropy input component form.
- If entered in entropy input component form, at least two components **shall** be entered by different users. The components **shall** be of equal length and format. Note that in this case, the cryptographic module **shall** separately authenticate the user entering each component. Documentation **shall** prove that if knowledge of n components is required to determine the entropy input to be used by the DRBG, then knowledge of n-1components provides no information about the final entropy input to be used other than its length.
- Entropy input that enters the cryptographic boundary (either encrypted or as entropy input components) **shall** move directly into the DRBG boundary without

Comment [ebb1]: Page: 1
This would preclude a single entity entering the the entropy input. This may be OK for banking and govt. applications, but may be too stringent for regular users. Leave as shall or change to should ? It's not anything that we can really enforce.

Comment [ebb2]: Page: 1
Do we want to say more about this ?

being stored, combined or otherwise processed by processes outside the DRBG boundary.

- Decryption of the encrypted entropy input or combining the entropy input components **shall** only be performed within the DRBG boundary.
- Other processes within the DRBG boundary **shall not** store, combine or otherwise process the entropy input.
- The resulting computed entropy input **shall only** be used to generate seed material.

8.4.3.3 Electronic Entry

When entered electronically, the entropy input is entered through the FIPS 140-2 cryptographic boundary into the DRBG boundary (see Section 8.2).

- The entry input **shall** be entered in encrypted form.
- Entropy input that enters the cryptographic boundary **shall** move directly into the DRBG boundary without being stored, combined or otherwise processed by processes outside the DRBG boundary.
  - Decryption of the encrypted entropy input **shall** only be performed within the DRBG boundary.
  - Other processes within the DRBG boundary **shall not** store, combine or otherwise process the entropy input.
  - The decrypted entropy input **shall only** be used to generate seed material.

8.4.3.4 Entry of Entropy Input from Within the Cryptographic Boundary Containing the DRBG Boundary

The entropy input for a DRBG (destination DRBG A) **may** be obtained from an NRBG, another DRBG (source DRBG B) or an entropy source contained within the same cryptographic boundary.
The source and destination for the entropy input **may** be contained within the same DRBG boundary. For example, an NRBG could be contained within DRBG A's boundary.
A cryptographic boundary may be disjoint. For example, DRBG A could reside in a FIPS 140-2 validated smart card, and DRBG B could be a separate entropy input provider. In normal operation, DRBG A and DRBG B would be considered as two separate cryptographic modules. However, during the entry of the entropy input into the smart card's DRBG, the combination of the two cryptographic modules could be considered as a single cryptographic module.

- The destination DRBG (DRBG A) **may** accept the entropy bits directly from the source DRBG (DRBG B) in plaintext, encrypted or entropy input component form.

The entropy input from the source DRBG (DRBG A) **shall not** be stored, combined or otherwise processed other than by the destinationDRBG.