

Below is the March 26, 2024 version of IG 9.3.A Resolution 2(b), for reference in the latest IG 9.3.A Additional Comment 12.

2. The module is passively receiving the entropy while exercising no control over the amount or the quality of the obtained entropy.

Examples include:

- (b) A software module that contains an approved DRBG that receives a LOAD command (or its logical equivalent) with entropy obtained from either inside the physical perimeter of the operational environment of the module or, via an I/O port, from an external source that is outside the module's physical perimeter.

What is required: (i) the SP **shall** state the minimum number of bits of entropy believed to have been loaded and justify the stated amount (from the length of the entropy field and from any other factors known to the vendor), (ii) the following caveat **shall** be added to the module's certificate: *No assurance of the minimum strength of generated SSPs (e.g., keys).*

If the amount of entropy used to generate the module's SSPs employed in an approved mode is *known to be* less than 112 bits, then this module cannot be validated.