Questions for Public Comment of SP 800-90B

1. This Recommendation does not allow for entropy sources with non-approved conditioning functions to provide full entropy. Can you provide any justification for why this should not be prohibited? Is there a test/set of tests that can be defined to test the output of these functions that is repeatable regardless of what conditioning function is used? [Section 6.2]

2. This Recommendation states that implementations using **approved** conditioning components may provide full entropy if an input string with at least 2*n* bits (or more) of assessed entropy is provided to an **approved** conditioning function with an *n*-bit output. However, it can be shown that there are cases in which this is not true (~1 bit of entropy can be lost by conditioning). This does not introduce a practical security loss, but does indicate that the claim is too strong. Are there any suggestions for handling this? Would a less stringent definition of full entropy allow for the intent without the problems with the security claim? [Section 6.4.2]

3. This Recommendation mandates that any conditioned output be IID, and will verify this via testing (for non-approved conditioning components). Is there an example of a (good) conditioning function that will produce non-IID data? Should non-IID testing be included in the testing of conditioned output? [Section 8.2]

4. This Recommendation requires that either the two specified continuous health tests be implemented, or tests that detect the same failure conditions. Validation testing of ‘equivalent’ tests is included, but no validation is specified for implementations of the required tests. How should the implementation of these tests be verified? Is it reasonable to request independent implementations of the health tests to check that the failure conditions are detected (regardless of the test used)? [Section 8.4]

5. Non-IID tests defined in this Recommendation have a fixed maximum symbol size, which means that they cannot provide an entropy estimate larger than that maximum. This is due to the data requirement stated earlier in the document. Would it be more reasonable to have the maximum symbol size computed dynamically, based on how much data has been provided? [Section 9.3]