Comments on X9.82, Part 1, dated May 18, 2005

From Elaine Barker, NIST

Note: The bolded text indicates issues for discussion.

1. Foreword, para. 1, line 5: Should "ASC" be "ASC X9" or "ANSI"? The same question applies to the use of "ASC" in para. 3 and 4.

   Para. 2, last line: Change "with" to "of".

2. Section 1, item 1 of the Part 4 list: indent the second line.

3. Section 2, line: Should "NIST" be inserted before "Cryptographic"?

4. Section 4.15, line 2: Change to "…security. Contrast…".

5. Section 4.48, line 3: **Change "80 bits" to something like "at least the number of bits equal to the security level".** [[This isn't linked to security level, it's linked to our magic number of "maximum innocent actions." The point is that it's okay to use some technique that doesn't allow repeating outputs, because repeating outputs have a negligible probability anyway, so the lack of repeating outputs doesn't let an attacker have a very good chance of distinguihsing the output from a random sequence.

   Suppose I have a DRBC which doesn't allow outputs to repeat, and my outputs are 80 bits wide. Then if I generate 2^{64} outputs, it's *easy* to distinguish my DRBC from an ideal rndom source, because with 2^{64} 80-bit outputs, the probability of not getting at least one repeated output from an ideal random source is really small.

   If the maximum number of outputs permitted is N, then our hypothetical DRBC must have a big enough output size that the probability of getting a repeated output from an ideal random source after N outputs is negligible. For N=2^{64}, that's about 160 bits. (The probability of getting two identical 160-bit outputs in 2^{64} tries is only about 2^{-33}.)

   We definitely need to discuss this in group!

   --JMK]]

   Formatted: Font: Bold

6. Section 6.1, para. 3, line 2: Change the semicolon to a comma. In line 3, change the comma to a semicolon.

   Para. beginning "Section 12…", line 2: Do we need the 2nd sentence here? I wouldn't think so. The same comment applies to the Section 13 text.

7. Section 6.3, item 4: Remove the 2nd sentence, since the X9.44 draft no longer specifies an RNG.

8. Section 7.2, Item 2: Indent the 2nd and 3rd lines. In the first line, place a space between "a" and "'1'".

   Table 2: Need to correct the right hand side of the table, as it's off the page.

   Para. beginning "As the above…", line 6: Insert "in Annex C" after "code". Line 7: Insert "above" before "example".

9. Section 7.3, item 1, line 8: Does "hidden coin" need to be changed to "hidden ideal coin"?
10. Section 8.2, item 2, line 4: Insert ", but will be unable to do so because of the backtracking resistance." After "concern", insert "for this example".

    Last para., line 8: Change "…DRBG," to "…DRBG that is".
11. Section 8.3, item 4: **Is this worded correctly? Do we really mean the health tests, which won't be very stringent? Or do we mean something like the NIST statistical tests? How does DRBG output relate to the health tests in Part 2?** [[We've commented on this before. Item 4 is a subset of Item 2. It doesn't hurt to add it, but if your RBG fails the statistical tests, then I can definitely distinguish it from random, b y running those statistical tests.]]
12. Section 8.4, item 3, line 2: **Does text like "before providing additional output" need to be placed after "entropy"?** [[It seems really odd to me to talk about this at the RBG level. Maybe the application can somehow recover, but the RBG can't, can it? A failure detected typically means that some major thing has gone wrong--the ring oscillator has stopped oscillating, or the AES engine isn't doing AES right anymore, or some such disaster. I'm having a hard time seeing how the RBG recovers from this!]]
13. Section 9.1, Figure title: Word is misbehaving; this should be Figure 1.
14. Section 9.2, para. 2, line 4: Change "is the coin flip" to "may be the results of the coin flip".

    Last 2 sentences: The last sentence is confusing. What about changing these two sentences to something like "The DRBGs in Part 3 of this Standard explicitly recognize their dependence on a source of entropy input, which could be, for example, from an NRBG or a properly initialized DRBG."

    Para. 4, line 7: Change "…to be an NRBG, which contains…" to "…to be from an NRBG, which is…".
15. Section 9.5, para. 1, last part of the 2nd sentence: **Figure 1 does not show that the OGF calls the ISTF.** [[I think the diagram is showing data flows, not control flows, so it's reasonable that it doesn't show this.]]
16. Section 9.8, last para.: **At the end of this para., there is a discussion of the relationship of security levels to NRBGs, but not to DRBGs. I suggest breaking this para. into 2 paragraphs, with the second para. starting after the 2nd sentence. Then add another para. about DRBGs, something like:**

    For DRBGs, the security level depends on the cryptographic primitive used (e.g., the hash function or block cipher algorithm), the key size (if appropriate) and the amount of entropy provided when instantiated and reseeded.
17. Section 10.2, last line: Capitalize "Standard".
18. Section 10.3, lines 1 and 4: Change "Additional Inputs" to "Other Inputs".
19. Section 10.6, item 3, sentence starting in line 7: **If "this process" is referring to the OGF, then the statement is in conflict with 9.5, which says that only the ISTF modifies the internal state. If "this process" is referring to the ISTF, then this sentence is repeating what was said in the first part of the previous sentence. The easiest solution might be to**

remove the sentence that starts in line 7. [[I commented on this, too. This is a silly requirement, and it breaks all our symmetric DRBGs.]]

20. Section 11.1, para. 1, line 4: **I suggest removing the last part of this sentence (the text after the comma), since it may not (and is probably not) true. Part 3 doesn't get entropy input in this way, though the Part 3 Get_entropy function could do so, i.e., for Part 3, this API is a lower level call. How does this relate to Part 2?** [[Yep, this is out of synch. I wonder if it even makes sense to have this in here. This is something that's got to be hashed out between parts 2, 3, and 4, but which shouldn't involve part 1 at all. --JMK]]
21. Section 11.1.3, 3rd line from the bottom of the pseudocode: 11.1.1 indicates that status is returned, but this line does not indicate it's return or the handling of an error status code.
22. Section 11.2: **Which of these functions is appropriate for DRBGs and which for NRBGs?**
    - **RBG_Instantiate and RBG_Uninstantiate are appropriate for a DRBG. Are they reasonable for an NRBG, in particular, for an enhanced NRBG?**
    - **RBG_Reseed is appropriate, but optional for a DRBG. What about for an NRBG?**
    - [[These were my comments, too.]]

    Comments and suggested text for each function are provided below.

Formatted: Font: Not Bold

Formatted: Bullets and Numbering

23. Section 11.2.1, Process: Change to something like "The security level is applicable to DRBGs and for some NRBGs. This parameter specifies…"

    Next para.: Change to something like "The prediction resistance supported flag is applicable to DRBGs. The flag indicates…".

    Full entropy supported flag para.: **The presence of this flag is still not clear to a new reader. Perhaps there should be some discussion in Part 4 with a reference to Part 4 placed here?** [[This kind-of breaks the DRBG/NRBG distinction in the rest of the document. I'm not sure what it (or really sections 11-12) are adding to Part 1.]]

    Para. on the personalization string: Change to something like "A personalization string is applicable to DRBGs; when used it is combined with…" **Is a personalization string appropriate for an enhanced NRBG?**

    Para. on RBG-specific parameters: Note that these are only needed for the Dual_EC_DRBG and the MS_DRBG. If they are not included in Part 3, these parameters can be omitted. Change to something like "RBG specific parameters are applicable to some DRBGs and enhanced NRBGs." Remove the last sentence.

    Handle: **Will the use of a handle be applicable to any type of NRBG?** If not, this needs to be stated. [[It's crazy to get into handles at this level of abstraction: they're basically about how these things are implemented.]]

24. Section 11.2.2: Again, **will the use of a handle be applicable to any type of NRBG?** If not, this needs to be stated.

    Para. on the security level: Change to something like "The security level is applicable to DRBGs and enhanced NRBGs. The security level parameter indicates the minimum security level for the output bits. If the DRBG has not…

Next para.: Change to something like "For DRBGs, if the …"

Full entropy requst para.: Again, **the use of this flag can be confusing. A reference to Part 4 for understanding the use of this flag might be appropriate.**

25. Section 12: Would it be better to place this section before Section 11, assuming that Section 11 is modified to discuss the difference in APIS when DRBGs and NRBGs are used?

26. Section 12.1, para. 1, line 4: **A DRBG does not provide full entropy.** [[A DRBG might accidentially provide full entropy. For example, if I call HMAC_DRBG using SHA256 with prediction resistance and use it to generate 128 bits of output, I get full entropy. But a DRBG doesn't promise this in general.]]

27. Section 12.2: **Do we need to talk about basic and enhanced NRBGs here? It might be appropriate to insert "when operating correctly" after "unbounded" in para. 1, line 8.** [[Yes, I think so too.]]

28. Section 12.3, line 2: Again, **A DRBG does not provide full entropy.**

    2nd sentence: **A DRBG doesn't have non-deterministic components; the RBG consisting of the DRBG and the source of entropy input, which has non-deterministic components somewhere up the line.** [[We need to discuss the terminology here: what's a DRBG, what's a DRBC Mechanism, what's a DRBC Algorithm, etc. Something an application will think of as a DRBG is providing it bits, and that thing had better have some kind of an ultimate entropy source!]]

    Para. 3, line 5, "an entropy source…": **Change to something like "a source of entropy input that is capable of providing sufficient entropy".**

29. Section 12.4: **Should this section be moved to Part 4?** [[Not sure. I don't see what it adds here, though.]]

    Item 2, line 3: Remove "potential".

    Item 3, lines 5-6: **None of the DRBGs have been designed to provide full entropy.**

    Item 4, 2nd sentence: **The DRBG is incapable of providing full entropy. Remove this sentence. Change the 3rd sentence to "The Enhanced NRBG is rated at the security level provided by the DRBG."** [[We need to discuss this security level question. If I can use a raw entropy source to instantiate AES-256-CTR-DRBG, why can't I use the entropy source embedded in an enhanced NRBG whose fallback security is based on AES-128-CTR-DRBG?]]

    Item 4, line 2: **Basic NRBG" isn't the right term. It could be a basic NRBG or a conditioned entropy source.**

30. Section 12.5: **Should this section be moved to Part 4?**

31. Section 13: **The editorial group recommends keeping at least some of this text here until such time as Part 4 is completed.**

    [John: Don't forget to check that this won't conflict with Part 4.]

    [[I think we'll be happier with this omitted from Part 1 and handled in Part 4. The big issue here is that this looks like a normative section, so if I put any additional requirements on combining RBGs (and I do), a designer may try to get their less secure

design in by complying with the normative text on combined RBGs in Part 1, rather than the more stringent normative text in Part 4.]]

32. Section 13.1: Should there be a note that this is not necessarily an Enhanced NRBG, even though it looks similar? **Note that in the 2nd para., an Enhanced NRBG is mentioned, but hasn't been discussed earlier.** [[This should all be in part 4, not here. But it's possible (with great care) to reuse the DRBG component of an enhanced NRBG for faster bits which aren't full-entropy. There are requirements Part 1 doesn't have and shouldn't mess around with here.]]

33. Section 14: Revise if the Dual_E_DRBG is not included in Part 3, since there will not be a need to convert an integer to a bit string. Also remove the appropriate sections and renumber, as appropriate.

34. Section 14.2.1, para. before the numbered items: Change to "as bit 4" and "as bit 1".

35. Section 15.1, para. 2: Note that the equivalent of a "stuck bit" test has been inserted into each DRBG after consulation with the CMVP director.

36. Section 15.3: **Basic and Enhanced NRBGs have not be discussed.**

37. Section 15.4, last para., line 4: Change "generating" to "the DRBG generates". Last line: Change "self-test processing" to "self-testing".

38. Annex A.2, last para., line 1: Capitalize "Part".

39. Annex A.4, para. 4, line 2: What does "this" refer to? Guessing an ideal *K*-bit random number?

40. Annex A.4.3, para. beginning "The answer is given…", line 7: Insert a "(" before "i.e.".

    Para. beginning "Interestingly…": Indicate why the min-entropy is still 2 bits by adding something like ", since the value (s) with the highest probability still has a probability of ¼, which can be expressed in two bits." [or whatever is appropriate to say]