X9.82, Part 3 Discussions during the teleconference:

Next draft to include:

1. 2 new hash-based DRBGs: KHF_DRBG and HMAC_DRBG
2. Revised Hash_DRBG to:
    - Provide backtracking resistance,
    - Eliminate the required application-specific constant t; such information can be provided in a personalization string
3. Possibly a block cipher-based DRBG
4. An un-instantiate process
5. Possibly an abort process for test failures and entropy input source failures

Operational testing specifications

- Will test each process (instantiation, generation, reseeding)
- Test diagrams will be removed, since they don't adequately show the testing process

6. Implementation considerations with respect to FIPS 140-2 cryptomodules
7. Discussion on DRBG selection
8. Expanded security considerations annex
9. Add Find_state_space function
10. Add Uninstantiate process to Hash_DRBG
11. Generic testing in Section 9
12. Specify the string lengths to be tested for each DRBG
13. Modify Hash_DRBG per John's suggestions
14. Usage_class -> state_pointer
15. Remove test diagrams for each DRBG
16. Non-secret input -> additional input
17. Section discussing why each DRBG should be chosen.
18. Entropy input source entropy >= requested strength requirements
19. Define Abort error handling function.
20. Provide a discussion of personalization strings.