Random Bit Generation Workshop
Agenda

December 5-6, 2012
NIST – Gaithersburg, MD

Day 1 (December 5th): SP 800-90B

Time	Agenda Item
9:00-9:15	Welcome and workshop purpose (Elaine Barker)
9:15-10:15	High-level presentation of SP 800-90B (John Kelsey)
10:15-11:15	Presentation of non-IID tests (Patrick Hagerty)
11:15-11:45	Break
11:45-12:15	General discussion of SP 800-90B (led by Mike Boyle) 1. Use of approved and non-approved conditioning components 2. Use of conditioning components to provide full entropy output. 3. Is there a conditioning component that will produce non-IID data?
12:15-1:00	Lunch
1:00-2:30	Collecting raw data (discussions led by John Kelsey) 1. Entropy Sources – Practical Designs and Validation Challenges (Sonu Shankar and David McGrew) 2. Other data-collection issues.
2:30-3:00	Break
3:00-5:00	Test discussions: 1. IID tests (John Kelsey) 2. Non-IID tests (e.g., should maximum symbol size be computed dynamically) (Patrick Hagerty) 3. Continuous (health) tests (e.g., the tests specified, and the use of equivalent tests) (John Kelsey) 4. Restart tests (John Kelsey) 5. Sanity tests (John Kelsey) 6. Dealing with test results (John Kelsey)

Random Bit Generation Workshop
Agenda

December 5-6, 2012
NIST – Gaithersburg, MD

Day 2 (December 6th): Validation

9:00-9:30	General CAVP and CMVP testing strategy –how testing will change (Mike Cooper)
9:30-10:00	CAVP testing -how validation testing is currently done for algorithms and the expected differences in validation testing for 800-90B entropy sources (Sharon Keller)
10:00-10:30	Envisioned transition strategy from old RNG requirements to SP 800-90 requirements (Mike Cooper)
10:30-11:00	Break
11:00-11:30	Test tool developed by the Australians (Tim Hall)
11:30-12:30	Current Testing/Validation issues (Sharon Keller)
12:30-1:15	Lunch
1:15-4:45 (includes a 30-minute break)	Testing SP 800-90B entropy sources (discussions led by Tim Hall) 1. Transition strategy, including current testing methodology vs. new methodology 2. Recognition of other testing programs 3. FIPS 140-2/3 annexes 4. Validation lists 5. DRBG/NRBG issues (using entropy sources with DRBG mechanisms)
	RBG construction issues (discussions led by Elaine Barker) 1. Using DRBG mechanisms from SP 800-90A
4:45-5:00	Closing (Elaine Barker)