Agenda
NIST Random Bit Generation Workshop
May 31 – June 1, 2023

All times are Eastern Time (New York)
(UTC –4)

Wednesday, May 31, 2023	
Session I – Moderator: Allen Roginsky	
10:00 – 10:10 10 min	***Opening Remarks*** *Matthew Scholl, Chief, Computer Security Division*
10:10 – 10:25 15 min	***Overview of NIST Random Number Generation Standards (90A, 90B, 90C, 22)*** *Meltem Sönmez Turan, NIST*
10:25 – 11:10 45 min	***SP 800-90C in Depth and Revision*** *Kerry McKay, NIST*
11:10 – 11:30 20 min	***NISTIR 8427 Full Entropy Definition*** *Darryl Buller, NSA*
11:30 – 12:00 30 min	***SP 800-90A in Depth and Revisions*** *Elaine Barker, NIST*
12:00 – 13:00	**BREAK**
Session II – Moderator: Chris Celi	
13:00 – 13:20 20 min	***Overview of ISO standards (ISO 18031 and 20543)*** *Gaëtan Pradel, INCERT*
13:20 – 13:50 30 min	***Overview of AIS 20/31*** *Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik (BSI)*
13:50 – 14:15 25 min	***Bridging the Gap Between the SP 800-90 Series and AIS 20/31*** *Kerry McKay, NIST*
14:15 – 14:40 25 min	***ASC X9: Revisions to ANS X9.82*** *Elaine Barker, NIST*
14:40 – 15:00 20 min	***CMUF Entropy Working Group*** *Lisa Rabe, Cisco*
15:00	**Adjourn for Day**

Thursday, June 1, 2023	
Session III – Moderator: Kerry McKay	
10:00 – 10:30 30 min	***SP 800-90B in Depth and Revision*** *Meltem Sönmez Turan, NIST*
10:30 – 10:55 25 min	***Use of Stochastic Models in RBG standards: Challenges and Opportunities*** *Johannes Mittman, Bundesamt für Sicherheit in der Informationstechnik (BSI)*
10:55 – 11:20 25 min	***Vendor CHTs*** *DJ Johnston, Intel Corporation*
11:20 – 11:45 25 min	***Lessons learned during Validation of 90B entropy sources (CMVP/CAVP) experiences*** *Tim Hall and Chris Celi, NIST*
11:45 – 12:10 25 min	***Non-physical entropy sources*** *Chris Celi and Tim Hall, NIST*
12:10 – 13:00	**BREAK**
Session IV – Moderator: Tim Hall	
13:00 – 13:25 25 min	***Health Tests for 90B*** *John Kelsey, NIST*
13:25 – 13:45 20 min	***DRBG Chains: RBGC Construction*** *John Kelsey, NIST*
13:45 – 14:00 15 min	***RBG3-RS Construction*** *John Kelsey, NIST*
14:00 – 15:00	***Open discussions and Closing Remarks***
15:00	**Adjourn**