From:	Miller, Carl A. (Fed)
To:	McKay, Kerry A. (Fed); Kelsey, John M. (Fed); Sonmez Turan, Meltem (Fed)
Subject:	Re: NIST SP 800-90 series
Date:	Wednesday, October 19, 2016 9:57:56 AM

Hi folks –
I'll just look for you all in our hallway (in the B-wing, bldg. 222) around 11:00am. See you then!
-Carl
————

Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

From: "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>
Date: Friday, October 14, 2016 at 7:56 AM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>
Subject: Re: NIST SP 800-90 series
That should work for me. SRR ends at 11.
-Kerry

From: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Date: Thursday, October 13, 2016 at 5:15 PM
To: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>, Kerry McKay <kerry.mckay@nist.gov>
Subject: Re: NIST SP 800-90 series
Hi John –
Ok, how about 11:00am on Wednesday (Oct. 19)?
Thanks for the list – that's indeed helpful. Talk to you later!
-Carl
————

Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

From: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
Date: Thursday, October 13, 2016 at 1:50 PM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>, "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>
Subject: Re: NIST SP 800-90 series
Everyone,
I know we have some people from the University of Maryland coming that afternoon, and a group picture at noon. I am free that morning, however.
The things NIST does related to randomness are:
a. The SP 800-90 work.

b. The FIPS 140 folks who oversee validation of crypto modules with RNGs.
c. The NIST Beacon
d. The NIST physicists who are working on quantum randomness, loophole-free Bell tests, etc.
e. We also have a publication on statistical testing of RNGs (testing against the model of iid unbiased bits).
--John

From: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Date: Thursday, October 13, 2016 at 12:29 PM
To: "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>, "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>
Subject: NIST SP 800-90 series

Hi John & Kerry –
Meltem and I were planning to meet to discuss the NIST SP 800-90 series (any anything else that our division does related to randomness). I'm interested in learning about the current state of the projects and possible ways to get involved. Is there any chance you might be interested in joining us? If so, Meltem mentioned Wednesday next week as a possibility – I'll be available 10am-2pm that day, and also 4:30-5:30pm. Talk to you later!
-Carl

———

Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD