From: Bassham, Lawrence E (Fed)
To: Perlner, Ray A. (Fed); Moody, Dustin (Fed); Alperin-Sheriff, Jacob (Fed)
Cc: Chen, Lily (Fed)
Subject: Re: Someone Is Testing Our DRBG requirements
Date: Friday, April 7, 2017 11:43:35 AM

Just let me know – or Dustin.

From: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Date: Friday, April 7, 2017 at 11:16 AM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Cc: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Subject: RE: Someone Is Testing Our DRBG requirements

Huh, AES 128 AES 192 and AES 256 CTR DRBG have seed lengths of 256, 320, and 384 bits respectively according to SP 800-90a, maybe we should use those values for the lengths of randombytes in our API.

From: Moody, Dustin (Fed)
Sent: Friday, April 07, 2017 10:36 AM
To: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: Someone Is Testing Our DRBG requirements

From their conclusion:

For generic implementations of discrete Gaussian sampling CTR-DRBG with AES is a safe option, particularly if AES hardware acceleration is available or you want to enter a NIST competition. It possesses a balance of performance and security, is well understood and is accepted by the security community.

I enjoyed the part "or if you want to enter a NIST competition".

From: Moody, Dustin (Fed)
Sent: Friday, April 7, 2017 10:28:35 AM
To: Alperin-Sheriff, Jacob (Fed); Perlner, Ray (Fed); Bassham, Lawrence E (Fed)
Cc: Chen, Lily (Fed)
Subject: Re: Someone Is Testing Our DRBG requirements

Sure. Just make it more of an email from you, and not an official NIST message from our PQC team.

They must have been already working on this.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Friday, April 7, 2017 9:14:46 AM
To: Moody, Dustin (Fed); Perlner, Ray (Fed); Bassham, Lawrence E (Fed)
Cc: Chen, Lily (Fed)
Subject: Someone Is Testing Our DRBG requirements

That was relatively fast given that we only just finished clarifying it.

https://eprint.iacr.org/2017/298

Can I reach out to them and let them know we're very happy to see this kind of work being done?

—Jacob Alperin-Sheriff