I'll look into it.

On: 17 April 2017 10:04, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:

Larry,

   I hope what we do is still compatible with the Open Quantum Safe project as well (https://openquantumsafe.org/). It says they use liboqs, which also includes common routines available to all liboqs modules, including a common random number generator and various symmetric primitives such as AES and SHA-3. Do they already have a NIST DRBG can you tell? From my un-expert eyes, it seems they might be using AES Ctr DRBG? See https://github.com/open-quantum-safe/liboqs

Dustin