From: Perlner, Ray (Fed)
To: Moody, Dustin (Fed)
Subject: Here"s text summarizing what we said in our meeting. Note that John will need to expand on his advice regarding "seed expander"
Date: Tuesday, July 18, 2017 5:16:40 PM

Q: How should submitters choose symmetric algorithms for their submissions?

A: While NIST will permit submitters to choose any NIST approved cryptographic algorithm for their submission if they feel it is necessary to achieve the desired security and performance, a number of potential submitters have asked us to offer default options for common symmetric cryptographic primitives. As such, here are our suggestions:

1. Hash functions: SHA512 is likely sufficient to meet the requirements of any of our five security strength categories and gives good performance in software, especially for 64 bit architectures. Submitters seeking a variable length output or good performance in hardware may instead prefer to use SHAKE256.
2. Authenticated encryption: We'd suggest AES256-GCM with a random IV.
3. KDFs: Where security proofs can accommodate something that is not indifferentiable from a random oracle, John's AES-based seed-expander will offer excellent performance. Otherwise, KMAC256 will be a good choice.