1161-68-301 **Daniel C Apon*** (daniel.apon@nist.gov). *Passing the final checkpoint! NIST PQC's 3rd Round begins.*

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere.

In response, NIST initiated a process in late 2017 to solicit, evaluate, and standardize one or more PKEs/KEMs and digital signature schemes. The Round 3 candidates were announced on July 22, 2020. This third round is expected to continue for another 12-18 months, at which point the initial post-quantum cryptographic standards are expected to be finalized and announced.

In this talk, I will survey the decision-making process of NIST in choosing its third round candidates – in particular, I will aim to explain NIST's thinking in choosing its finalists for near-term standardization.

Further, I will highlight a variety of issues and open questions that NIST believes are the most important to answer in this next year and a half before the first post-quantum cryptographic standards are chosen. (Received August 18, 2020)