The NCCoE Migration to PQC project offers a panel presentation or presentations during which we will share our progress and insights gained from our work with our collaborators. Our project seeks to ease the Migration to PQC. We have focused on cryptographic discovery and on interoperability and performance of the draft algorithms in selected communication protocols.

1) The panel presentation or presentations will offer insights gained as we collaborated to publish following draft publications:

NIST SP 1800-38B, Quantum Readiness: **Cryptographic Discovery**, is a preliminary draft offering (1) a functional test plan that exercises the cryptographic discovery tools to determine baseline capabilities; (2) a use case scenario to provide context and scope our demonstration; (3) an examination of the threats addressed in this demonstration; (4) a multifaceted approach to start the discovery process that most organizations can start today; and (5) a high-level architecture based on our use case that integrates contributed discovery tools in our lab.

NIST SP 1800-38C, Quantum Readiness: **Testing Draft Standards for Interoperability and Performance**, is a preliminary draft offering (1) identification of compatibility issues between quantum ready algorithms, (2) resolution of compatibility issues in a controlled, non-production environment, and (3) reduction of time spent by individual organizations performing similar interoperability testing for their own PQC migration efforts.

2) The panels will also discuss future directions for the project and share progress in our labs made since the drafts were posted and since new collaborators joined the project.

Primary Submitter:
Bill Newhouse, NIST/ITL/ACD/NCCoE, newhouse@nist.gov
100 Bureau Drive STE 2002
Gaithersburg MD 20899-2002

Co-Submitter
Murugiah Souppaya, NIST/ITL/CSD, murugiah.souppaya@nist.gov
100 Bureau Drive STE 8930
Gaithersburg MD 20899-8930