From:	David A. Cooper
To:	Dworkin, Morris J. (Fed); Dang, Quynh H. (Fed); Miller, Carl A. (Fed); Davidson, Michael S. (Fed); Apon, Daniel C. (Fed)
Subject:	Reference for quantum resistance of hash functions
Date:	Wednesday, August 14, 2019 3:41:06 PM

I did some searching for a reference for the text at the end of Section 1. One possibility would be to reference NISTIR 8105, *Report on Post-Quantum Cryptography* (https://doi.org/10.6028/NIST.IR.8105). It doesn't have much text on the subject, but its probably enough to justify the assertion in our text.

Dave