From:	Hall, Timothy A. (Fed)
To:	Dworkin, Morris J. (Fed); Vassilev, Apostol T. (Fed)
Cc:	Hall, Timothy A. (Fed)
Subject:	RE: Review of draft SP 800-208 and responses to public comments
Date:	Monday, June 22, 2020 9:37:36 AM

Hi Morrie,

Thank you for sending these. I will review the documents and get comments back to you. Best,

Tim

From: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Sent: Monday, June 22, 2020 9:25 AM
To: Vassilev, Apostol T. (Fed) <apostol.vassilev@nist.gov>; Hall, Timothy A. (Fed) <timothy.hall@nist.gov>
Subject: Review of draft SP 800-208 and responses to public comments

Good morning, Apostol and Tim,

The PQC team is close to finalizing SP 800-208, which profiles the IETF specifications of stateful hash-based signatures for NIST approval. Attached for your review are the latest drafts of both the document itself and our proposed responses to the public comments. We would welcome your feedback, especially on the several requirements in the Conformance section that are most relevant to the validation programs. Feel free to distribute the documents to anyone else in your group that you think is appropriate.

I would be grateful if we could receive any comments you might have by July 2, or just let me know if you'd like more time.

Thanks,

Morrie