From: Moody, Dustin (Fed)
To: Kerman, Sara J. (Fed)
Cc: Dworkin, Morris J. (Fed)
Subject: Small typo regarding hash-based signatures
Date: Wednesday, August 28, 2019 9:41:12 AM
Attachments: NIST 2nd PQC Workshop talk.pptx

Sara,

A few small corrections to make. Somebody noticed that when we talk about stateful hash-based signatures we transposed two digits in one of the RFC's. We mention RFC 8931, when it should be RFC 8391. I've corrected it on my slides for the presentation I gave at the workshop last week (attached). Also, he noted two pages on our websites:

The pages concerned are:

https://csrc.nist.gov/projects/stateful-hash-based-signatures
https://www.nist.gov/news-events/news/2019/02/request-public-comments-stateful-hash-based-signatures-hbs

No rush to fix this. Thanks!

Dustin