From: Wallner, Debbie M <dmwalln@tycho.ncsc.mil>
Sent: Monday, July 07, 2014 11:27 AM
To: internal-hash
Subject: Comments on Draft FIPS 202
Attachments: Comments on Draft FIPS PUB 202 dated April 2014.docx

Please accept these comments on Draft FIPS PUB 202.

NSA Comments on Draft of FIPS PUB 202, dated April 2014

Page 1, Section 1, Footnote 4: Consider changing "relatively small" to "sufficiently small". For example, if the output length for SHAKE128 is d = 224, the collision security is 112 bits, which is smaller than 128. Thus, this is an example of an "exception" as alluded to in the footnote. As such, it suggests that an output size of d = 224 must therefore be "relatively small". However, d = 224 is the output size of SHA3-224, one of the hashes specified in this very standard, so it would seem somewhat odd to classify this output size as being "relatively small". A similar discussion is applicable to SHAKE256 with output length d = 384 (i.e., the footnote would seem to suggest that d = 384 is a "relatively small" output size, when in fact it's the output size for one of the four hashes specified in the standard).

Various sections: Make sure when defining the state array, the limits of the parameters are $0 <= x < 5$, $0 <= y < 5$, and $0 <= z < w$. Incorrect limits are given in sections 3.1 (last paragraph), 3.1.2 (2^{nd} paragraph), 3.1.3 (definitions of Lane(i,j) and Plane(j)), 3.2.1 (Algorithm 1), 3.2.3 (Algorithm 3), 3.2.4 (Algorithm 4), and 3.2.5 (Algorithm 6).