**From:** Moody, Dustin (Fed)
**To:** Cooper, David (Fed); Kelsey, John M. (Fed); internal-pqc
**Subject:** Re: Terminology
**Date:** Thursday, June 25, 2020 2:52:08 PM

---

I can see that it is confusing, even though it makes sense to me.

Anybody else have any other options besides "alternates", "alternate candidates", or "additional candidates"?

---

**From:** David A. Cooper <david.cooper@nist.gov>
**Sent:** Thursday, June 25, 2020 2:47 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
**Subject:** Re: Terminology

I think using "candidates" to refer specifically to those algorithms advancing to the third round, but not as finalists, is confusing. We've been using the term "candidate" since the CFP to refer to all submissions that are still under consideration. In the current report we say that the process started with "69 candidate algorithms," and say that there are "26 second round candidate algorithms." It would be very confusing to then, when talking about the third round say that "candidate" means algorithms that have not been eliminated but that are not finalists.

Rather than overloading the term "candidate," I think it is much better to separate the algorithms moving on to the third round as finalists and alternates (or alternate candidates). If there is concern that "alternate candidates" has negative connotations, we could replace it with something like "additional candidates." But, trying to use "candidates" to refer to just the alternates will be confusing given all of the other uses in the report of "candidates" to refer to all remaining algorithms.

On 6/25/20 2:32 PM, Moody, Dustin (Fed) wrote:

> John,
> I tried to unify this. I put in a couple of sentences that the 7 finalists are called "finalists" and that other 8 advancing on are called "candidates". We often add an adjective to the candidates, such as "additional candidates" or "alternate candidates". Did you find somewhere where "candidates" is being used to apply to the finalists?
>
> Dustin
>
> ---
>
> **From:** Kelsey, John M. (Fed) <john.kelsey@nist.gov>
> **Sent:** Thursday, June 25, 2020 2:22 PM
> **To:** internal-pqc <internal-pqc@nist.gov>
> **Subject:** Terminology

Everyone,

I'm going over the document again after not looking at it for a few days. One problem I keep noticing—we do not have consistent terminology for our track 1 candidates, our track 2 candidates, and for all the stuff in round 2.

The best terminology I've seen in our document for this is:

a. Track 1 candidates are "finalists."
b. Track 2 candidates are "alternates,"
c. All the algorithms in the second round are "candidates."

We can always put "algorithm" after that term—"finalist algorithm" or "alternate algorithm" or "candidate algorithm." But I think we'd be much more clear if we tried to stick to this (or some other) consistent terminology for the different algorithms across the whole document. I keep seeing places where we use slightly different terminology for them in different sections (probably because each of us uses slightly different terminology).

Thanks,

--John