

**From:** (b) (6)  
**To:** [Apon, Daniel C. \(Fed\)](#)  
**Subject:** Re: Fw: Reminder: PKC subreviews (prefer them by this Monday, the 18th)  
**Date:** Friday, October 22, 2021 1:05:42 PM

---

Hi, Daniel,

I submitted it.

It was exactly what I thought. Every detail. I recommend acceptance because nobody has published something like this observation before.

Pretty sure it is the GeMSS team, though.

BTW, it was my idea and I told them about it at the beginning of round 3 for them to tweak their scheme and make it more efficient for signing. I mentioned explicitly in an email to them that you could reduce signature size even to below the security bound if the hash function is slow enough... lol

Anyway, it is science that is correct and has some interest.

Cheers,  
Daniel

On Fri, Oct 22, 2021 at 8:25 AM Daniel Smith (b) (6) wrote:  
hmmm..... Forgot about this one. Not interesting as I recall from reading the title. Maybe I can read more than the title and then repeat what I said before. I'll try this morning.

On Thu, Oct 21, 2021, 9:41 PM Apon, Daniel C. (Fed) <[daniel.apon@nist.gov](mailto:daniel.apon@nist.gov)> wrote:

---

**From:** Apon, Daniel C. (Fed) <[daniel.apon@nist.gov](mailto:daniel.apon@nist.gov)>  
**Sent:** Thursday, October 21, 2021 9:41 PM  
**To:** Smith-Tone, Daniel C. (Fed) <[daniel.smith@nist.gov](mailto:daniel.smith@nist.gov)>  
**Subject:** Re: Reminder: PKC subreviews (prefer them by this Monday, the 18th)

ree

---

**From:** Apon, Daniel C. (Fed) <[daniel.apon@nist.gov](mailto:daniel.apon@nist.gov)>  
**Sent:** Wednesday, October 20, 2021 8:16 PM  
**To:** Apon, Daniel C. (Fed) <[daniel.apon@nist.gov](mailto:daniel.apon@nist.gov)>  
**Subject:** Re: Reminder: PKC subreviews (prefer them by this Monday, the 18th)

Hi all,

It's ~8pm (Eastern) on Wednesday -- all reviews are due by 5pm Friday.

In order to ensure that all reviews are in on time, this is the **final call** -- please submit your reviews by 3pm Thursday. Otherwise, I will add the outstanding reviews to my pile of reviews to complete by 5pm Friday.

Your reviews do not have to be perfect; I am planning to review the reviews before finalized for the PKC peer-review process. You just need to write a few paragraphs and choose some scores. This is entirely up to you (and I highly doubt I'll edit things, unless it seems way out of scope somehow).

Please note that everyone BCC'd on this email thread is a NIST employee ( ); get it done!

--Daniel

P.S. Please let me know Thursday morning ASAP if you have problems with uploading your review

---

**From:** Apon, Daniel C. (Fed)

**Sent:** Friday, October 15, 2021 12:14 PM

**To:** Apon, Daniel C. (Fed) <[daniel.apon@nist.gov](mailto:daniel.apon@nist.gov)>

**Subject:** Reminder: PKC subreviews (prefer them by this Monday, the 18th)

Hi all,

Just a reminder that PKC reviews are due soon. I have a relatively large bucket of them to do on my own this next week, and I also need to do passes over any subreviews before forwarding them as official reviews.

I think I suggested this upcoming Monday (the 18th) for subreviews to be sent in

If you need a little extra time, or if you need any help in doing your review, please let me know

(The hard deadline for all final reviews is 1 week from today)

Also, disregard this email if you already sent yours in =)

Thanks so much,

--Daniel