

**From:** [Kerman, Sara J. \(Fed\)](#)  
**To:** [Foti, James \(Fed\)](#)  
**Cc:** [Moody, Dustin \(Fed\)](#)  
**Subject:** NISTIR 8413 -- FW: NPS: ERB Chair Review Manuscript  
**Date:** Wednesday, March 30, 2022 9:26:41 AM

---

Jim (+ Dustin)

I wanted you to be aware of this (see below) because it will determine if you prepare the final PDF or if I send it to the library for property checks. The pub will likely be ERB approved today, but until we get the lawyer green light, we won't publish.

Sara

---

**From:** Moody, Dustin (Fed) <dustin.moody@nist.gov>  
**Sent:** Wednesday, March 30, 2022 9:17 AM  
**To:** Kerman, Sara J. (Fed) <sara.kerman@nist.gov>  
**Subject:** Re: NPS: ERB Chair Review Manuscript

Thanks for confirming.

At our PQC meeting yesterday, **we did discuss adding a sentence or two**. The reason is that we are aware of a paper that will be published publicly any day now. The authors sent us a copy to review, so we know about it. Once it's published publicly, we can cite it, and need to have a sentence or two addressing its results. If it isn't published publicly before we announce, we don't need to add the sentences.

Dustin

---

**From:** Kerman, Sara J. (Fed) <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>  
**Sent:** Wednesday, March 30, 2022 9:14 AM  
**To:** Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
**Subject:** RE: NPS: ERB Chair Review Manuscript

Yes, Jim knows not to publish without your permission. I did mention yesterday that there was an approval from the lawyers needed before we could publish. So even if the pub is ERB approved, it may be held waiting on lawyers.

**(b) (6)**. If publishing takes place while he is on vacay, I will coordinate with the library to publish 8413 and Patrick is set to post the Announcement and Publication on CSRC.

Is the PDF you uploaded to NPS today **final** (i.e., ready for Jim to prepare for library posting)? Assuming we hear nothing from ERB Secretariat (which is rare)?

Sara

---

**From:** Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
**Sent:** Wednesday, March 30, 2022 9:06 AM  
**To:** Kerman, Sara J. (Fed) <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>  
**Subject:** Re: NPS: ERB Chair Review Manuscript

Yeah, she had acronyms for most of her comments. We have a table of acronyms to help with that.

(b) (5)  
[Redacted]

[Redacted]

---

**From:** Kerman, Sara J. (Fed) <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>  
**Sent:** Wednesday, March 30, 2022 9:03 AM  
**To:** Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
**Subject:** RE: NPS: ERB Chair Review Manuscript

(b) (5)  
[Redacted]

[Redacted]

---

**From:** Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
**Sent:** Wednesday, March 30, 2022 8:55 AM  
**To:** Kerman, Sara J. (Fed) <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>  
**Subject:** Re: NPS: ERB Chair Review Manuscript

Sara,

Okay, I went through and changed some things in accordance with her comments. I didn't change everything she wanted - hope that's fine. I uploaded this newer version to the system.

Dustin

---

**From:** Kerman, Sara J. (Fed) <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>  
**Sent:** Wednesday, March 30, 2022 8:19 AM  
**To:** Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
**Subject:** FW: NPS: ERB Chair Review Manuscript

Hey Dustin,

FYI - use discretion when deciding whether to implement Sheryl's comments. They are not required,

but it's good look through in case she caught something. Some editorial punctuation probably conflicts with Isabel's editing style (which is consistent in our pubs).

Sara

---

**From:** [no\\_reply@nist.gov](mailto:no_reply@nist.gov) <[no\\_reply@nist.gov](mailto:no_reply@nist.gov)>  
**Sent:** Tuesday, March 29, 2022 7:53 PM  
**To:** Sharpless, Katherine E. (Fed) <[katherine.sharpless@nist.gov](mailto:katherine.sharpless@nist.gov)>  
**Cc:** Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>; Kerman, Sara J. (Fed) <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>; Taylor, Sheryl L. (Fed) <[sheryl.taylor@nist.gov](mailto:sheryl.taylor@nist.gov)>  
**Subject:** NPS: ERB Chair Review Manuscript

**You have been selected to review the manuscript listed below:**

**Title:** Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process  
**Author Name(s):** Alagic Gorjan; Cooper David A.; Dang Quynh; Dang Thinh; Kelsey John M.; Lichtinger Jacob; Liu Yi-Kai; Miller Carl A.; Moody Dustin; Peralta Rene; Perlner Ray; Robinson Angela; Smith-Tone Daniel; Apon Daniel  
**Date Submitted:** 3/4/2022  
**ERB Control Number:** G2022-0854 **Comments:** [See comments in manuscript.](#)

*(Note that the previous reviewer and/or the author have been cc'd on this e-mail to make them aware of the change in the manuscript's status.)*

You can login to the NIST Publications System to view this manuscript at:  
<https://tsapps-i.nist.gov/nps/npsui>.

Please access the application, review the document, and add comments and a marked-up version of the manuscript if you've created one. You can approve the paper as it is, approve it with suggested changes, or return it to the author for mandatory changes. (When the author uploads a new version to address mandatory changes, you will be notified and given another opportunity to review and approve.)

Reviews are conducted to ensure that the quality management objectives for our publications are met in order to maintain NIST's reputation. All reviewers have specific responsibilities. The Group Leader ensures that the paper is ready for further review, evaluating its technical, and editorial quality as well as policy considerations. Technical reviewers read primarily for quality of technical content but can also assess editorial quality and compliance with policy. The Division Chief reads for technical and editorial quality and for policy compliance. The sponsor reads primarily to ensure compliance with policy but also for technical and editorial quality. Guidance for reviewers is available at <https://inet.nist.gov/files/pdf/guideforauthorsandreviewers>.

Once your work is completed, signal that you are finished by clicking on the appropriate button.

**Instructions for reviewing:**

- Go to <https://tsapps-i.nist.gov/nps/npsui>
- On the dashboard, click on the appropriate record to open it.
- In the center of the page, you can choose "Manuscript Details," "Comments," etc. Select "Document Management" and scroll down for a link to the paper.
- Review the paper and either upload a marked up copy of the manuscript, upload a separate document containing comments, or make a general comment.
- Approve the paper as is, approve it with suggested changes, or return it to the author for mandatory changes.
- The system will tell the authors that you've completed your review and will notify the next reviewers in line that it's their turn. You will be cc'd so you know that your action has been completed.

Please reply to [erbchair@nist.gov](mailto:erbchair@nist.gov) if you have any questions/comments.

**Thank you!**

**NIST Publications System (NPS) Administrators**