

From: [Chen, Lily \(Fed\)](#)  
To: [Regenscheid, Andrew \(Fed\)](#); [Moody, Dustin \(Fed\)](#)  
Subject: Re: New IP text?  
Date: Friday, July 29, 2016 2:14:09 PM  
Attachments: [image001.png](#)

Andy:

Thanks for update. We will get there. I am on my way back. See you Monday.

Lily

On: 29 July 2016 10:07, "Regenscheid, Andrew (Fed)" <[andrew.regenscheid@nist.gov](mailto:andrew.regenscheid@nist.gov)> wrote:  
No, not yet...

Henry keeps saying he'll get it to us. Last night he said "first thing in the morning," which has turned into "sometime today." I've been having the other lawyers up there poke him for us whenever they see him today.

Sara knows this might be something we need to finish on Monday morning. While certainly far from ideal, I think we handle that fine so long as there isn't a big problem with whatever text Henry provides.

-Andy

From: Chen, Lily (Fed)  
Sent: Friday, July 29, 2016 12:54 PM  
To: Moody, Dustin (Fed); Regenscheid, Andrew (Fed)  
Subject: New IP text?  
Hi, Andy and Dustin:

Have we received the text from Henry yet? (I might have missed an e-mail or so).

Lily

From: Dustin Moody <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
Date: Friday, July 29, 2016 at 8:03 AM  
To: "Regenscheid, Andrew (Fed)" <[andrew.regenscheid@nist.gov](mailto:andrew.regenscheid@nist.gov)>  
Cc: "Kerman, Sara J. (Fed)" <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>, Lily Chen <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)>  
Subject: RE: Per our discussion

Andy,

Yes, I think the intent was that the Background section would serve as an intro, but I can see what you are saying. I think it's a good idea to flip the order of the two. I think we want to make sure people know we want comments back on this, and so putting the RFC first should help with that. Do you think we need to add a pointer back to the FRN in our three paragraph RFC as shown on picture of the webpage Sara included below?

Dustin

From: Regenscheid, Andrew (Fed)  
Sent: Thursday, July 28, 2016 2:25 PM  
To: Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
Cc: Kerman, Sara J. (Fed) <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>  
Subject: Re: Per our discussion  
Dustin,

Maybe you can explain the reasoning for this. Sara showed me the PQC site earlier today. It seems strange to insert the "Request for Comments" in the middle- basically it's jammed between the first and second sections of the CFP. Was there a particular reason for that? Would it make more sense to flip the order in the navigation bar? Or include the Request for Comments at a top level page for PQC Standardization? Or was the intent that the Background section of the CFP would serve as an introduction on the website?

-Andy

From: "Kerman, Sara J. (Fed)" <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>  
Date: Thursday, July 28, 2016 at 1:14 PM  
To: Andrew Regenscheid <[andrew.regenscheid@nist.gov](mailto:andrew.regenscheid@nist.gov)>  
Cc: "Moody, Dustin (Fed)" <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
Subject: Per our discussion

Let me know what you and Dustin decide on the location of the RFC link:

Call for Proposals = Section 1 of CFP

Submission Reqs = Section 2 of CFP

...and so on through Evaluation Process = Section 5 of CFP

pqc.comments@nist.gov, with subject line 'Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria'. A red box highlights 'Do we need line regarding FRN' and a blue box highlights 'DRAFT Call for Proposals'."/>

File Edit View History Bookmarks Tools Help  
NIST.gov - Computer Security ... x ServiceNow x user BRC-Biometric Conferman... x Multicast Delayed Authenti... x jchalpin | NIST Cyber Com... x DHS Class of 1986 - 25 Year... x Verizon | My Verizon | Veri... x NIST Bibliography Web Ap... x  
file:///C:/csrc\_working/groups/ST/post-quantum-crypto/rfc-july2016.html  
information sciences peralta  
C SRC HOME > GROUPS > CT > POST-QUANTUM CRYPTOGRAPHY PROJECT  
POST-QUANTUM CRYPTO STANDARDIZATION  
Request For Comments On Submission Requirements And Evaluation Criteria  
The National Institute of Standards and Technology (NIST) is requesting comments on a new process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are specified in FIPS 186-4, Digital Signature Standard, as well as special publications SP 800-56A, Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography and SP 800-56B, Revision 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography. However, these algorithms are vulnerable to attacks from large-scale quantum computers (see NISTIR 8195, Report on Post-Quantum Cryptography).  
As a first step in this process, NIST is publishing draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms to solicit public comment. It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available royalty-free worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.  
The draft requirements and evaluation criteria are available in the menu to the left. The public comment period closes on September 16, 2016. Send comments to [pqc.comments@nist.gov](mailto:pqc.comments@nist.gov), with subject line "Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria".  
Do we need line regarding FRN  
DRAFT Call for Proposals  
NIST Cyber Vulnerability Disruption Mitigation & Strategic Policy  
NIST is an Agency of the U.S. Department of Commerce  
Last updated: July 28, 2016  
Page created: February 29, 2016

Sara J. Kerman  
NIST  
301-975-4634  
[sara@nist.gov](mailto:sara@nist.gov)