From: Moody, Dustin (Fed)
To: Kerman, Sara J. (Fed)
Subject: RE: Per our discussion
Date: Friday, July 29, 2016 8:28:00 AM
Attachments: image001.png

None that I have received!

From: Kerman, Sara J. (Fed)
Sent: Friday, July 29, 2016 8:27 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Per our discussion

Still no sign of the CFP from the lawyers?

From: Moody, Dustin (Fed)
Sent: Friday, July 29, 2016 8:03 AM
To: Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>
Cc: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>; Chen, Lily (Fed) <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>
Cc: Kerman, Sara J. (Fed) <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

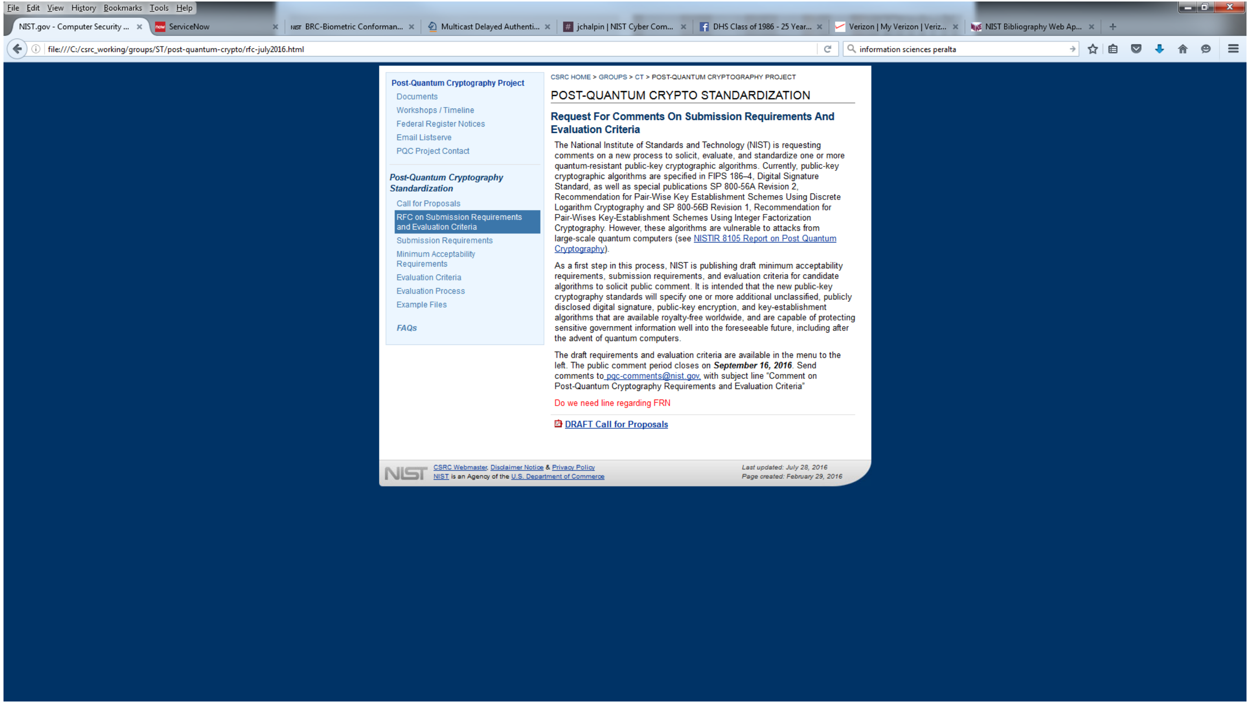
From: "Kerman, Sara J. (Fed)" <sara.kerman@nist.gov>
Date: Thursday, July 28, 2016 at 1:14 PM
To: Andrew Regenscheid <andrew.regenscheid@nist.gov>
Cc: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: Per our discussion

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


File Edit View History Bookmarks Tools Help
NIST.gov - Computer Security ...
ServiceNow
BRC-Biometric Conforman...
Multicast Delayed Authenti...
jchalpin | NIST Cyber Com...
DHS Class of 1986 - 25 Year...
Verizon | My Verizon | Veriz...
NIST Bibliography Web Ap...
file:///C:/csrc_working/groups/ST/post-quantum-crypto/rfc-july2016.html
information sciences peralta

Post-Quantum Cryptography Project
- Documents
- Workshops / Timeline
- Federal Register Notices
- Email Listserve
- PQC Project Contact

Post-Quantum Cryptography Standardization
- Call for Proposals
- RFC on Submission Requirements and Evaluation Criteria
- Submission Requirements
- Minimum Acceptability Requirements
- Evaluation Criteria
- Evaluation Process
- Example Files

FAQs

CSRC 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-Wises Key-Establishment Schemes Using Integer Factorization Cryptography. However, these algorithms are vulnerable to attacks from large-scale quantum computers (see NISTIR 8105 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, with subject line "Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria"

Do we need line regarding FRN

DRAFT Call for Proposals

CSRC Webmaster, Disclaimer Notice & Privacy 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