From: Scholl, Matthew (Fed)
To: Evans, Heather M. (Fed)
Subject: Re: need quick review - your challenges
Date: Friday, October 28, 2016 6:28:24 PM

Heather
Thanks and let me know if you need more

-------- Original Message --------
From: "Evans, Heather (Fed)" <heather.evans@nist.gov>
Date: Fri, October 28, 2016 6:21 PM -0400
To: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Subject: Re: need quick review - your challenges

Okey doke. It was all from material you all put online so it shouldn't be an issue.... thanks!

On: 28 October 2016 17:18, "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov> wrote:
The rest looked good to me.

From: "Evans, Heather (Fed)" <heather.evans@nist.gov>
Date: Friday, October 28, 2016 at 5:00 PM
To: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Subject: RE: need quick review - your challenges

Thanks will do. You still looking over the rest of the text?

From: Scholl, Matthew (Fed)

Sent: Friday, October 28, 2016 4:55 PM

To: Evans, Heather (Fed) <heather.evans@nist.gov>

Subject: Re: need quick review - your challenges

Heather,

Thanks. I prefer to call it an opportunity!

OK, so I am not too sure on authorities but FISMA 2002 and FISMA 2014 are good citations as they give NIST the authority to make standards for use by the USG, FIPS. I would add Federal Information Security Modernization Act (FISMA) of 2014.

From: "Evans, Heather (Fed)" <heather.evans@nist.gov>
Date: Friday, October 28, 2016 at 4:34 PM
To: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Subject: need quick review - your challenges

Hi Matt,

See below – this is the information I need to submit on your challenge. I am not going to do a full writeup on the other one because it looks like the workshop was in October so FY 17. We can cover it next year! Two quick requests of you:

(1) Is FISMA authority also relevant to the lightweight crypto project?
(2) Please take a look at the text below and make any edits.

Would be great to hear from you next week.

Thanks,

Heather

The Post-Quantum Crypto Project

Title	Post-Quantum Crypto Project
Sponsoring Agency	NIST
Prize Authority	No prize. Proposals collected pursuant to the Federal Information Security Management Act (FISMA) of 2002, Public Law 107–347.
Primary Point of Contact	Matt Scholl, matthew.scholl@nist.gov, 301-975-2941
Link	http://csrc.nist.gov/groups/ST/post-quantum-crypto/
Federal Register Notice	8/2/16 See https://www.federalregister.gov/documents/2016/08/02/2016-18150/request-for-comments-on-post-quantum-cryptography-requirements-and-evaluation-criteria
Submissions Opened	
Submissions Due	
Winners Announced	In process
Phases (Additional dates)	Call for proposals expected in Fall 2016, deadline for submissions in November 2017, Workshop for participants to present their submissions in early 2018. Analysis phase expected to last 3 – 5 years wherein NIST will report findings and hold 1-2 workshops. Draft standards anticipated 2 years after NIST's analysis is completed.
Submissions (#)	
Entrants (#)	
Participants (#)	-
Number of Prizes (#)	
Winners (#)	
Total Prize Purse ($$)	
Individual Awards ($$)	
Non-Monetary Incentives	
Operational Cost paid by Agency ($$)	
Estimated Value of Partner Contributions ($$)	
Estimated Investment Made by Solvers/ Teams ($$)	-

1. Problem Statement.

The Post-Quantum Crypto Project is an effort by NIST to solicit, evaluate, and standardize quantum-resistant public-key cryptographic algorithms by working closely with the cryptography community. A key part of this effort will be an open collaboration with the public, which will be invited to devise and vet cryptographic methods that—to the best of experts' knowledge—will be resistant to quantum attack. In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the internet and elsewhere. The goal of post-quantum cryptography (also called quantum-resistant

cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

In August 2016 NIST issued a request for comments in the Federal Register on a new process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. The document provided preliminary evaluation criteria for quantum-resistant public key cryptography standards. The criteria will include security and performance requirements. The comment period closed on September 16, 2016. After the document is finalized, NIST will begin accepting proposals for quantum-resistant public key encryption, digital signatures, and key exchange algorithms. NIST intends to select at least one algorithm providing each of these functionalities for standardization. NIST will establish a submission deadline late in 2017 for algorithms to be considered, allowing the proposals to be subject to 3 to 5 years of public scrutiny before they are standardized.

NIST expects that the evaluation process for post-quantum cryptosystems may be incredibly complex. It may not be possible to make a well-supported judgment that one candidate is "better" than another. NIST will perform a thorough analysis of the submitted algorithms in a manner that is open and transparent to the public, as well as encourage the cryptographic community to also conduct analyses and evaluation. This combined analysis will inform NIST's decision on the subsequent development of post-quantum standards.

2. Solutions Type.

Software and apps
Creative (design & multimedia)
Ideas
Technology demonstration and hardware
Nominations
Business plans
X Analytics, visualizations, algorithms
X Scientific
Other (please specify)

3. Proposed Goals.

The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. NIST's Post-Quantum Crypto Project aims to incentivize cryptography experts to develop and assist in the vetting of these systems.