From:	Apon, Daniel C. (Fed)
To:	Clark, Carol A. (Fed)
Cc:	Chen, Lily (Fed)
Subject:	RE: 60NANB18D217 Florida Atlantic University Board of Trustees - Technical Report- Response requested by Dec 6th
Date:	Tuesday, December 10, 2019 3:41:00 PM

- Is the description of the work for the current reporting period within the scope of the funded project?

Yes. The original proposal was in two parts: (1) setting up a wiki-style website for NIST PQC submissions, tracking various data (name, functionality, hardness assumption, parameters, security issues, official comments, etc.) and updating it as the rounds progress;
and (2) providing a collection of challenge problems, i.e. small-scale, properly-generated instances of the core problems underlying various schemes, and also proposal-specific challenges where appropriate.

During this reporting period, the FAU team finished setting up the wiki with the data as was described/promised for part (1), and it is online now. They've also advertised their wiki page at several international conferences so that it's known by and useful to the scientific community. Additionally, they've begun collecting and setting up the computational challenges for part (2); glancing at their website, they appear to have linked to a few other websites that have 'core computational challenges' as well as posted a proposal-specific set of challenges for ThreeBears.

- Are you satisfied with the work described in the technical report for the current period?

Overall, yes. Getting the intial wiki page online (with initial information about every NIST PQC candidate) is a major step, and in line with the proposed work.

Some links to previous, known challenge pages are missing. For example, I'm aware of two places that have lattice reduction or RLWE challenges: (i) https://web.eecs.umich.edu/~cpeikert/rlwe-challenges/ as well as (ii) https://www.latticechallenge.org/ (which has challenges for SVP, Ideal Lattices, and LWE).
It would be good to either link to these pages, or add their own challenges (according to whichever criteria seems most relevant to the NIST submissions, as they see fit), or both.

Also, as mentioned in the proposal "Keeping the entries up-to-date will be fundamental" -- along with this, it would be incredibly useful to have this Wiki record a list of every ePrint paper (or other paper) on the topic of each given scheme, in a list. For example, the pq-crystals.org page lists a new paper "Kyber on Cortex-M4" (Ref: https://eprint.iacr.org/2019/489),
and it would be nice to just keep a running list of EVERY paper for EVERY scheme sorted on the Wiki. The initial collection will be the most challenging, and perhaps the "broader community with write access" will contribute too, but once this is set up, it should be easy to update the page anytime something is posted to ePrint that is NIST PQC related.
(In principle, this could only be papers about specific schemes, or there could be a separate list for NIST-PQC-related paper links, e.g. on the topic of failure boosting attacks, which affects many

schemes at once.)
In any case, having this information on the wiki would certainly help it be a "one-stop-shop" for getting up to speed as a "newcomer" to the NIST PQC standards process.

That said, I would re-mention: I am happy with the progress that has already been made in the current period.

From: Clark, Carol A. (Fed)
Sent: Monday, December 9, 2019 3:12 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: 60NANB18D217 Florida Atlantic University Board of Trustees - Technical Report-Response requested by Dec 6th

Your review does not need to be lengthy .   If you have additional feedback, comments or concerns that absolutely fine.   Otherwise answering the questions is sufficient.

This financial assistance award was issued as a grant, and not a cooperative agreement.   In short that means NIST/ITL/you are not working collaboratively on the scope of work and providing input on the work.   However, if you have concerns they are conducting work that is not within the scope, they are not making adequate progress, etc. that is different.

I need to leave for the day, but would be happy to discuss tomorrow.   Feel free to give me a call.

Carol
X2239

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Monday, December 9, 2019 2:59 PM
To: Clark, Carol A. (Fed) <carol.clark@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: 60NANB18D217 Florida Atlantic University Board of Trustees - Technical Report-Response requested by Dec 6th

One quick question:

Is there any format of my review that I should try to adhere to (outside of the two questions you put in bullet points earlier in this email chain)?

For your information-- I have heard of this project previously, and been generally happy with its effect, but (if memory serves) there are a few things I would like to suggest to both NIST's

PQC team (if it can accommodate) and to the technical team at Florida Atlantic. I could include both of these in my review. However, I will at least first check around with the relevant parties at NIST about whether the NIST side of my suggestions/recommendations is possible.

(Outside of a few recommendations for (minor) additional work from the relevant parties, I expect I will review the outcomes here positively so far.)

--Daniel

From: Clark, Carol A. (Fed) <carol.clark@nist.gov>
Sent: Monday, December 9, 2019 2:53 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: 60NANB18D217 Florida Atlantic University Board of Trustees - Technical Report- Response requested by Dec 6th

Understood. Thanks Daniel. Let me know if you have any questions.

Carol

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Monday, December 9, 2019 2:52 PM
To: Clark, Carol A. (Fed) <carol.clark@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: 60NANB18D217 Florida Atlantic University Board of Trustees - Technical Report- Response requested by Dec 6th

P.S. Apologies for delays while I get up to speed!

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Monday, December 9, 2019 2:51 PM
To: Clark, Carol A. (Fed) <carol.clark@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: 60NANB18D217 Florida Atlantic University Board of Trustees - Technical Report- Response requested by Dec 6th

Hi Carol, thanks-- I will attend to this within this afternoon, if possible.
At latest, I will send this to you by Tuesday afternoon (tomorrow).

--Daniel

From: Clark, Carol A. (Fed) <carol.clark@nist.gov>
Sent: Monday, December 9, 2019 8:01 AM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>

Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: FW: 60NANB18D217 Florida Atlantic University Board of Trustees - Technical Report-Response requested by Dec 6th

Hi Daniel,

Please complete your review as soon as possible. The DOC Grants and Cooperate Agreements Manual allots a maximum of 30 days to evaluate progress reports from the date they are submitted. Completing the review is a critical monitoring tool.

Let me know if you have any questions.

Thank you,

Carol

From: Clark, Carol A. (Fed)
Sent: Friday, November 22, 2019 8:29 AM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: 60NANB18D217 Florida Atlantic University Board of Trustees - Technical Report-Response requested by Dec 6th

Good morning Daniel,

Thank you for agreeing to serve as the technical point of contact for this award.

I have attached the technical progress report from Florida Atlantic University, project "A Platform for the Evaluation of Post-Quantum Primitives" for the period 4/1/19-9/30/19. I have also attached the original proposal to assist with your review.

Some questions to guide your review:

- Is the description of the work for the current reporting period within the scope of the funded project?

- Are you satisfied with the work described in the technical report for the current period?

Please provide your feedback by Dec 6th.

I am available if you have any questions.

Thank you.

Carol Clark
Administrative Specialist/Federal Program Officer
Information Technology Laboratory
National Institute of Standards and Technology
Phone: (301) 975-2239
Email: carol.clark@nist.gov

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Thursday, November 21, 2019 2:55 PM
To: Clark, Carol A. (Fed) <carol.clark@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: 60NANB18D217 Florida Atlantic University Board of Trustees - New Technical Point of Contact

Sure.. I can do this. Let me know what the future steps are.

--Daniel

From: Clark, Carol A. (Fed) <carol.clark@nist.gov>
Sent: Wednesday, November 20, 2019 8:34 AM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: 60NANB18D217 Florida Atlantic University Board of Trustees - New Technical Point of Contact

Good morning Daniel,

Lily has provided an excellent summary of the responsibilities of a technical point of contact. I have provide a few additional actions below:

- Review the semiannual progress reports to ensure they align with the original proposal - critical monitoring function
- Approve the reports or provide reasons for disapproving the reports to facilitate my request for a revised report
- Review any changes requested by Florida Atlantic University during the award period and provide your input

Please let me know if you are able to serve as the technical point of contact. I have included a copy of the original proposal and the current progress report to permit you to make your decision.

I will provide specific questions for your review if you accept the responsibility.

Thank you,

Carol

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Tuesday, November 19, 2019 6:02 PM
To: Clark, Carol A. (Fed) <carol.clark@nist.gov>
Cc: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Re: 60NANB18D217 Florida Atlantic University Board of Trustees - New Technical Point of Contact

Hi, Carol,

I would like to suggest Daniel Apon as technical point of contact, unless he has a conflict.

Hi, Daniel,

Can you please serve as the technical point of contact for the award? The duty includes reviewing progress report.

Thanks,

Lily

On: 20 November 2019 05:20, "Clark, Carol A. (Fed)" <carol.clark@nist.gov> wrote:

> Hi Lily,
>
> Can you please provide a replacement technical point of contact for Jacob Alperin-Sheriff for the Florida Atlantic University Board of Trustees award 60NANB18D217 "A Platform for the Evaluation of Post-Quantum Primitives"? The semi-annual report has been submitted for review.
>
> Thank you,
>
> *Carol Clark*
> Administrative Specialist/Federal Program Officer
> Information Technology Laboratory
> National Institute of Standards and Technology
> Phone: (301) 975-2239
> Email: carol.clark@nist.gov