Hi, Carol,

Thanks. I am satisfied with the modified report.

Lily

From: Clark, Carol A. (Fed)
Sent: Wednesday, April 24, 2019 4:39 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: Award # 60NANB16D246 - Performance Progress Florida Atlantic University- Approval Requested by May 8th

Hi Lily,

I have attached the revised technical progress report from Florida Atlantic University for the period 10/1/18-3/31/19, along with the original proposal to assist with your review.

Please let me know if you are satisfied with the revised report.

A response by May 8th would be appreciated.

Thank you.

Carol

From: Clark, Carol A. (Fed)
Sent: Tuesday, April 23, 2019 3:05 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: Award # 60NANB16D246 - Performance Progress Florida Atlantic University- Approval Requested by May 3rd

Thank you Lily.   I will request a revised report, per your suggestion.

I will be in touch when the revised report is received.

Carol

From: Chen, Lily (Fed)
Sent: Tuesday, April 23, 2019 1:14 PM

To: Clark, Carol A. (Fed) <carol.clark@nist.gov>
Subject: RE: Award # 60NANB16D246 - Performance Progress Florida Atlantic University- Approval Requested by May 3rd

Hi, Carol,

I looked at the progress report. Thank you for noticing SIKE performance. In general, we hope the recipients will use the grants to investigate a category of candidates for standardization not a single candidate. But it happens that SIKE is the only candidate in one category. I think that "investigated the performance of SIKE on ARMv7 devices" can be considered as the relevant activities and results for the awarded grants. But "submitting SIKE Round 2 to the NIST standardization process" should not. In fact, I do not think submit round 2 version would not cost much of the resource for the specific team, if you know the team which submitted SIKE is quite large.

That is said, I think we might approve the progress report with comments such as
---
The Grants are intent to support research on the proposed topics not generating NIST submissions, even those are often a part of the research. The submission teams to NIST PQC Standardization are supposed to be self-sponsored. It is not NIST intention to support some but not others. Please revise the report accordingly.

From: Clark, Carol A. (Fed)
Sent: Friday, April 19, 2019 1:49 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Award # 60NANB16D246 - Performance Progress Florida Atlantic University- Approval Requested by May 3rd

Good afternoon Lily,

I have attached the technical progress report from Florida Atlantic University for the period 10/1/18-3/31/19.   I have also included the original proposal to assist with your review.   The original proposal outlined in detail the proposed work, project plan and schedule. I believe it would have been helpful to have a similar level of detail in the technical report.   Much of the accomplishment section is boiler plate information.

Does investigated the performance of SIKE on ARMv7 devices and/or submitting SIKE Round 2 to the NIST standardization process fit within the scope of their proposed work/project plan?

Please let me know if you are satisfied with the report and the research documented in the report.

A response by May 3rd would be appreciated.

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