From: Scholl, Matthew (Fed)
To: Evans, Heather M. (Fed)
Cc: Regenscheid, Andrew R. (Fed)
Subject: RE: Quick review - OSTP prizes report
Date: Wednesday, March 29, 2017 5:51:12 PM

Thanks. I would say "international acclaim in the field of Cryptography" but perhaps bragging rights is easier understood

-------- Original Message --------
From: "Evans, Heather (Fed)" <heather.evans@nist.gov>
Date: Wed, March 29, 2017 1:59 PM -0400
To: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
CC: "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>
Subject: RE: Quick review - OSTP prizes report

Hi Matt,

First – yeah that is correct about the PQC. The report includes a more detailed description of PQC that we wrote. The excerpt I sent is from some front material that OSTP wrote. I will add a comment and propose the text in red (I don't know if they'll take it) …

"In running a prize competition, managers sometimes develop clearer success metrics and validation protocols than current industry standards in order to evaluate solutions submitted by applicants. These new methods for measurement can create new ways to evaluate solvers and solutions head-to-head, both for the prize competition and the technology more broadly. The NIST *Post-Quantum Crypto Project* challenge seeks to leverage ~~this~~ the benefit of competition (in this case, offering bragging rights) in order to establish standards for public-key cryptographic algorithms that are resistant to large-scale quantum computers. NIST is currently accepting proposals through late 2017 and intends to select at least one algorithm providing quantum-resistant public key encryption, digital signatures, and key exchange algorithms for standardization. Proposals will be subject to three to five years of public evaluation before they are standardized."

Thanks for the heads up on the ONC writeup. I will tell them to remove the word "attendance" – the funds were to support the workshop. But I did get word back from conf services that the amount is correct.

From: Scholl, Matthew (Fed)
Sent: Wednesday, March 29, 2017 12:32 PM
To: Evans, Heather (Fed) <heather.evans@nist.gov>
Cc: Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>
Subject: Re: Quick review - OSTP prizes report

Heather

I don't have much context on this but while the PQC work is a "competition" in that we will select some winners, there is no prize award with the selection of a submitted algorithm. I don't want to give the impression that there is a prize with PQC.
We helped with the conference facilities fees and not the prize awards for the conference with HHS. I would check with Conference Facilities for the budget that was covered.
Matt

From: "Evans, Heather (Fed)" <heather.evans@nist.gov>
Date: Wednesday, March 29, 2017 at 10:52 AM
To: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Cc: "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>
Subject: Quick review - OSTP prizes report

Matt,

I need a really quick review of 2 areas in the final version of OSTP's prize competition report. Can you take a look and get back to me ASAP? Thank you!!

"In running a prize competition, managers sometimes develop clearer success metrics and validation protocols than current industry standards in order to evaluate solutions submitted by applicants. These new methods for measurement can create new ways to evaluate solvers and solutions head-to-head, both for the prize competition and the technology more broadly. The NIST *Post-Quantum Crypto Project* challenge seeks to leverage this benefit in order to establish standards for public-key cryptographic algorithms that are resistant to large-scale quantum computers. NIST is currently accepting proposals through late 2017 and intends to select at least one algorithm providing quantum-resistant public key encryption, digital signatures, and key exchange algorithms for standardization. Proposals will be subject to three to five years of public evaluation before they are standardized."

Also – can you tell me who from NIST was involved with the ONC Blockchain Challenge? (I thought maybe Andy?) HHS included some info about it that talks about NIST's engagement on the challenge; for diligence I want to make sure it's accurate. This is pretty simple, just need to know if this is right:

"an estimated $3,000 was provided by NIST for supporting the workshop attendance."

Heather

Heather M. Evans, Ph.D.
Program Coordination Office
Office of the Under Secretary for Standards & Technology, and NIST Director
National Institute of Standards and Technology (NIST)
Telephone: 301-975-4525
Mobile: 240-863-8628