From: Chen, Lily (Fed)
To: Dodson, Donna F (Fed); Regenscheid, Andrew R. (Fed)
Cc: Scholl, Matthew A. (Fed)
Subject: RE: annual report welcome letter
Date: Tuesday, May 23, 2017 11:42:06 AM

Donna:

It reads good.

Lily

From: Dodson, Donna F (Fed)
Sent: Tuesday, May 23, 2017 11:40 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>
Cc: Scholl, Matthew (Fed) <matthew.scholl@nist.gov>
Subject: Re: annual report welcome letter

Does this look ok:

Looking ahead is vital in the realm of cybersecurity. Knowing that if large-scale quantum computers are ever built they will be able to break many of the public-key cryptosystems currently in use and compromise the confidentiality and integrity of digital communication on the Internet and elsewhere, NIST is working closely with the academic community and industry to develop protective cryptographic standards that we all rely upon. Building on its successful tradition of working openingly with the worldwide cryptographic community, in 2016 NIST called for submissions for quantum-resistant public-key cryptographic algorithms for standards. These algorithms must be secure against both quantum and classical computers, and should interoperate with existing communications protocols and networks. After submissions are received late in 2017, NIST plans to spend 3-5 years to work with research community and industry to analyze the candidates before selecting algorithms for standardization.

From: Lily Chen <lily.chen@nist.gov>
Date: Thursday, May 18, 2017 at 4:41 PM
To: "donna.dodson@nist.gov" <donna.dodson@nist.gov>, Andrew Regenscheid <andrew.regenscheid@nist.gov>
Cc: Matthew Scholl <matthew.scholl@nist.gov>
Subject: Re: annual report welcome letter

Hi, Donna:

This looks good. I have two comments and one suggestion as attached.

Lily

From: "Dodson, Donna F (Fed)" <donna.dodson@nist.gov>
Date: Thursday, May 18, 2017 at 2:35 PM
To: Lily Chen <lily.chen@nist.gov>, "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>
Cc: Matthew Scholl <matthew.scholl@nist.gov>
Subject: annual report welcome letter

Lily and Andy,

In the welcome letter for the annual report, we include a highlight on the post quantum crypto work:

Looking ahead is vital in the realm of cybersecurity. Knowing that if large-scale quantum computers are ever built they will be able to break many of the public-key cryptosystems currently in use and compromise the confidentiality and integrity of digital communication on the Internet and elsewhere, NIST is working closely with the academic community and industry to develop protective cryptographic standards that we all rely upon. Building on its successful tradition of worldwide, open competitions, in 2016 NIST called for submissions for quantum-resistant public-key cryptographic algorithms for standards. These algorithms must be secure against both quantum and classical computers, and should interoperate with existing communications protocols and networks. NIST plans to select a winning entry after all entries are received late in 2017 and thoroughly analyzed.

The basis for these words came some of your posted material. It has been edited a few times though so would you take a look and let me know if you have any changes?

Thanks,

Donna