From: Chen, Lily (Fed)
To: Regenscheid, Andrew (Fed); Dodson, Donna F (Fed)
Subject: RE: IPR policy AES vs. SHA-3
Date: Friday, July 8, 2016 2:25:00 PM

Andy:
You are correct. What I have was published in the January 2, 1997, which is the draft for comments. That is, it is dropped that option in the final announcement. Actually I was surprised to see the second option " b) available under terms consistent with ANSI patent policy".
Lily

From: Regenscheid, Andrew (Fed)
Sent: Friday, July 08, 2016 1:28 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Dodson, Donna F (Fed) <donna.dodson@nist.gov>
Subject: Re: IPR policy AES vs. SHA-3

Are you sure AES allowed an ANSI-like IPR statement?
I've attached a copy of the AES call for algorithms. While they apparently initially were going to allow an ANSI IPR policy statement, pressure during the comment period on the draft submission requirements caused them to change the requirement to royalty-free in the final call.
Andy

On: 07 July 2016 06:48, "Chen, Lily (Fed)" <lily.chen@nist.gov> wrote:

Thanks a lot.
Lily

From: Dodson, Donna F (Fed)
Sent: Wednesday, July 06, 2016 9:36 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: (b) (6) Burr, William E. (Assoc) <william.burr@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>
Subject: Re: IPR policy AES vs. SHA-3

Let's call ginger in the morning to set a time with Chuck because Lisa is out this week

On: 06 July 2016 19:38, "Chen, Lily (Fed)" <lily.chen@nist.gov> wrote:

I printed Henry's email, voltage letter, and AES FRN, as well as Ajit' comments. Thanks for help.
I will be in the office the rest of the week. Any time works for you and Chuck will work for me.
Shall I send an email to Lisa?
Lily

On: 06 July 2016 17:53, "Dodson, Donna F (Fed)" <donna.dodson@nist.gov> wrote:
Thanks much – I recall the ANSI discussion for AES. We did think about the international questions when we put that requirement in place.

Let’s try to talk with Chuck this week.

From: Lily Chen <lily.chen@nist.gov>
Date: Wednesday, July 6, 2016 at 12:57 PM
To: "donna.dodson@nist.gov" <donna.dodson@nist.gov>
Cc: (b) (6) Bill Burr <william.burr@nist.gov>, Andrew Regenscheid <andrew.regenscheid@nist.gov>
Subject: FW: IPR policy AES vs. SHA-3

Hi, Donna:

I talked with Bill today. He does not remember why we dropped “ b) available under terms consistent with ANSI patent policy” in SHA-3 competition. It seems at that time people are willing to go with RF. Bill was not involved in the drafting FRN for AES.

Lily

From: Chen, Lily (Fed)
Sent: Tuesday, July 05, 2016 3:26 PM
To: Burr, William E. (Assoc) <william.burr@nist.gov>; (b) (6)
(b) (6)
Cc: Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Dodson, Donna F (Fed) <donna.dodson@nist.gov>
Subject: IPR policy AES vs. SHA-3

Hi, Bill:

I think Andy may have talked with you about the comments we received from Ajit on our IPR handling in call for submissions of Post-Quantum Cryptography algorithms. Today, when I talked with Donna, I first time realized that for AES, we actually allow two options: a) freely available b) available under terms consistent with ANSI patent policy. For SHA-3, as we stated in FRN, we only allow 2) – “Should my submission be selected for SHA-3, I hereby agree not to put any restrictions on the use of the algorithm intending to be available on a worldwide, non-exclusive, royalty-free basic. “ Do you remember why we dropped option 2) in SHA-3? Or is my understanding wrong? Thanks,

Lily