From: Regenscheid, Andrew (Fed)
To: Scholl, Matthew A. (Fed); Chen, Lily (Fed); Dodson, Donna F (Fed)
Subject: Re: QRC Stall
Date: Thursday, June 30, 2016 6:01:54 PM

Matt, +Donna,

Lily and I met with OCC and Ajit earlier today.

As you may recall, the sticking point is over the draft call's requirement for submitters to agree to worldwide, royalty-free licensing terms. Ajit is concerned that such a statement may harm the US position in trade negotiations, citing cases where another country has effectively required companies to give up IP rights to sell into that market.

Basically, Ajit is interpreting our IPR clause as saying: "to gain access to the USG market, you must give up your IPR on your product (the crypto algorithm)." I think Henry and Ajit know this isn't quite the same situation, but they're concerned nonetheless.

Henry suggested that we instead follow ANSI's model where tell submitters that they must provide letters of assurance stating what IP terms they're agreeing to, whether that be royalty-free, RAND, or perhaps something in the middle. Then we would include IPR terms in the evaluation of the proposals, with a stated preference for submissions agreeing to RF terms.

To some extent, this would be a more formal version of what's been done with block cipher modes. Henry points out what this would still allow us to get what we want at the end of the process, without creating a hard rule up-front. That's potentially true, however, it's hard to predict how the crypto community would respond. I would expect strong push back from the academic community, as well as the Internet standards community, on any signal that we're moving away a commitment to RF for fundamental crypto standards. Would these individuals and groups stay involved and simply advocate for the submissions that come with RF terms, or would they decide it is simply not worth their effort to participate if there's a chance we'd ultimately select encumbered algorithm? Would it have an impact on where people focus their evaluation efforts? Or, would IPR become a major distraction throughout the evaluation process, drawing attention away from technical evaluations on security and performance?

We don't know what would happen.

Henry's office is going to propose alternative language. However, I don't think there's much we could do in that language that would strongly mitigate the concerns above, other than stating a preference for RF, which might not be strong enough.

Thoughts? Could we get verification from someone that asking for RF really does create a trade negotiations problem?

Regards,
Andy

From: Matthew Scholl <matthew.scholl@nist.gov>
Date: Monday, June 27, 2016 at 9:44 AM
To: Lily Chen <lily.chen@nist.gov>, Andrew Regenscheid <andrew.regenscheid@nist.gov>
Subject: QRC Stall

Lily and Andy,

Thank you for working with the program office and the GC on getting the QRC FRN out.

I understand the concerns that Ajit has expressed but I have some thoughts here.

1. This is an issue of national importance that has many variables outside of our control. For us to introduce

an issue that will delay implementation is unacceptable for me.
2. We know that allowing encumbered submissions Will Delay implementation. This is the lesson of ECC.
3. It is essential for industry to implement Before the catastrophic occurrence of a practical quantum computer defeats all our PKI. We know from experience that industry will not implement if there are IP issues without a catastrophic issue. This is the lesson of DES still in state/local law enforcement infrastructures.
4. Based on “guessed” Q Day, the IC community is already moving to halt any future crypto migrations until QRC is available. For the IC, we are late.

I want you to get the FRN out this month (June). I apologize for being out on leave during this conversation. If the program office wants to hold the FRN and/or wants us to include IP in submissions, Elevate This Issue Immediately to Donna with a recommendation that Chuck intervene.

Chuck is fully read into this issue from all angles and will be helpful if we need him.

Thank you

Matt