From: Bohn, Robert B. (Fed)
To: Chen, Lily (Fed)
Subject: Re: FW: [csa-announcements] Quantum-Safe Security Glossary Peer Review
Date: Thursday, September 29, 2016 9:37:25 AM

Dear Lily,

Hi there. I want to thank you for your thoughtful and well written response. In my role in the cloud program in ITL, I am constantly exposed to new concepts and considerations. I realize there is a great & significant importance associated with cryptography and its utility when applied to computer security.

I should also say that I do know much about this field but I would like to ask you if you have suggestions or a publication list that I can peruse to try to do some catching up. I don't plan on becoming an expert, but I should have a basic understanding of concepts and techniques.

Thanks!

-b

==========

Robert Bohn, PhD
NIST Cloud Computing Program Manager
NIST
100 Bureau Drive
Gaithersburg, MD
20899-2000
Phone: 301-975-4731
http://www.nist.gov/itl/cloud

From: Chen, Lily (Fed)
Sent: Wednesday, September 28, 2016 1:11:28 PM
To: Bohn, Robert B. (Fed); Boisvert, Ronald F (Fed)
Cc: Jordan, Stephen P (Fed); Mink, Alan (Assoc)
Subject: RE: FW: [csa-announcements] Quantum-Safe Security Glossary Peer Review

Hi, Ron and Bob:
Thank you for the information. We are aware Cloud Security Alliance's approach. There is a report at 4th ETSI/IQC Workshop on Quantum-Safe Cryptography last week by Bruno Huttner from IDQuantique last week. There are some other organizations developing guidelines or standards about "Quantum-Safe Cryptography", either classical cryptography resistant to quantum attacks or quantum key distributions such as ETSI and IETF, besides CSA. Each organization has its own timeline and moves on some specific categories. For example IETF has some drafts for hash based signature. NIST will develop standards for generic usage and will consider the other standard activities to understand their usage. For that reason, we like to know all the activities. But we are focus on crypto primitives and will not get into protocol levels.
It will be hard to synchronize. But we will try. Thank you for sending the information.
Lily

From: Bohn, Robert B. (Fed)
Sent: Wednesday, September 28, 2016 10:16 AM
To: Boisvert, Ronald F (Fed) <boisvert@nist.gov>
Cc: Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Mink, Alan (Assoc) <alan.mink@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: FW: [csa-announcements] Quantum-Safe Security Glossary Peer Review

Ron,
Thanks for passing this on to Lily & Al. ☺
I can only speculate that CSA wants to be the 1-stop shop for cloud security needs and has decided that their group needs to put a stake in the ground regarding the topic of security for quantum computing.
-bob

From: Ronald Boisvert [mailto:ronald.boisvert@nist.gov]
Sent: Wednesday, September 28, 2016 10:11 AM
To: Bohn, Robert B. (Fed) <robert.bohn@nist.gov>
Cc: Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Mink, Alan (Assoc) <alan.mink@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: FW: [csa-announcements] Quantum-Safe Security Glossary Peer Review

Dear Bob,

Not sure why we need another working group on this topic, but perhaps if what they are doing is trying to interpret trends in this area to make them understandable to the cloud community, then I suppose that is helpful.

I have cc-d two other ITL folks on this: Lily Chen, who leads the Cryptography Group in CSD and Alan Mink of ACMD who tracks developments in QKD.

Ron

On 9/28/2016 9:54 AM, Bohn, Robert B. (Fed) wrote:

> Dear Stephen & Ron,
> We do some work with the CSA and they are expanding their interests to include quantum computing. I am forwarding this link to you and perhaps you would also like to offer some comments on this work.
> I have not participated in this specific group, but it looks like a mass email.
> -bob
> **From:** csa-announcements-bounces+robert.bohn=nist.gov@lists.cloudsecurityalliance.org [mailto:csa-announcements-bounces+robert.bohn=nist.gov@lists.cloudsecurityalliance.org] **On Behalf Of** CSA Announcements List
> **Sent:** Tuesday, September 27, 2016 12:23 AM
> **To:** Research <research@cloudsecurityalliance.org>
> **Subject:** [csa-announcements] Quantum-Safe Security Glossary Peer Review
>
> > Dear Colleagues,
> > The Cloud Security Alliance would like to invite you to review and comment on the Quantum-Safe Security working group's latest document, Quantum-Safe Security Glossary. This document is the latest in a series of documents from the working group introducing quantum computing. This document is intended to help the industry understand quantum-safe methods for protecting their networks and their data and increase quantum-safe awareness . This glossary collects the main terms used in quantum-safe cryptography.
> > This is your opportunity to provide feedback and identify any critical areas that we might be missing in the document's focus. The open review and comments period starts today and ends on October 31th, 2016. Follow the below link to the peer review site to begin the process to submit feedback:
> > https://docs.google.com/document/d/17lcOZyjcw4aWV_9snJhJoKUjs6deprtxNDGTG19AJD0
> > Thank you in advance for your time and contribution and we appreciate your involvement. If you are interested in getting involved with this working group, please register on the Quantum-Safe Security microsite registration page.
> > Thank you,
>
> --
> Ryan Bergsma
> Research
> Cloud Security Alliance
> CloudSecurityAlliance.org
> c-rbergsma@CloudSecurityAlliance.org
> 360-739-4441