From: Scholl, Matthew (Fed)
To: Boutin, Chad T. (Fed)
Subject: Re: Lightweight crypto news coverage
Date: Monday, April 22, 2019 12:23:11 PM

Chad
How do I get someone added to the daily news clips? Steve Lipner from my FACA board had requested and Chuck approved.

-------- Original Message --------
From: "Boutin, Chad T. (Fed)" <charles.boutin@nist.gov>
Date: Mon, April 22, 2019 9:38 AM -0400
To: "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>, "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>
CC: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Subject: Lightweight crypto news coverage

FYI Inside Cyber's story from April 19 remains their #1 trending article as of this morning.
CB

NIST seeks comment on 'lightweight' encryption for IoT devices

April 19, 2019 |
Rick Weber

The National Institute of Standards and Technology is requesting public comment on several dozen "lightweight cryptography" proposals issued Thursday, which are intended to support secure Internet of Things devices.

"As the next step in its effort to create effective security for small networked electronic devices, [NIST] is requesting feedback from the public on the set of 56 candidate 'lightweight cryptography' proposals the agency released today," **according to a statement** issued by NIST.

NIST is expecting to pare down the number of proposals beginning this fall, while viewing the overall cryptography effort as an iterative process.

"NIST scientists are particularly interested in feedback concerning the overall security of the candidates, as well as their performance and suitability for specific applications," according to the statement. "The NIST team will use comments received before September 2019 to winnow the group of 56 down to a smaller set of candidates, and the team will continue to accept comments after this smaller set is announced."

The latest proposal is the result of cryptographic algorithms submitted by developers in response to a request from NIST last year.

“The goal is to develop cryptographic standards that can work within the confines of simple electronic devices with limited circuitry, such as those used in Internet of Things networks. Common encryption methods may demand more electronic resources than these tiny devices possess,” according to NIST.

The issue of cryptography came up at a NIST advisory board meeting in March during which NIST IT lab Director Charles Romine **voiced concerns about China's push** toward quantum computing and its potential ability to crack encryption codes.

"It's interesting from the impact it has on the community but also from a historical perspective, we cut our teeth on cybersecurity in the cryptography space," Romine said at the March 20-21 meeting of the NIST Information Security and Privacy Advisory Board. -- *Rick Weber* (***rweber@iwpnews.com***)
9842