From: Boutin, Chad T. (Fed)
To: Chen, Lily (Fed); Scholl, Matthew A. (Fed); Dworkin, Morris J. (Fed)
Subject: RE: For review / FW: Cryptography topic page
Date: Monday, October 25, 2021 4:38:08 PM

Thanks again Lily! I'll make minor tweaks if any.

CB

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Monday, October 25, 2021 4:36 PM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>; Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Subject: RE: For review / FW: Cryptography topic page

Hi, Chad,

Let me try to tweak a little bit. You may further tweak it.

Key establishment, which involves establishing the keys among communication parties used for data protection (or information protection), using public-key cryptography.

Lily

From: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Sent: Monday, October 25, 2021 4:25 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Subject: RE: For review / FW: Cryptography topic page

Thanks Lily. I'll change the sentence to read "continues to lead public collaborations" to avoid confusion. I'll also incorporate digital signatures as part of the hash bullet and revise the bullet order per your below.

Is this bullet OK for key establishment?

Key establishment, which involves generating the keys used in some cryptographic systems, including public-key cryptography.

CB

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Monday, October 25, 2021 3:50 PM
To: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>; Boutin, Chad T. (Fed) <charles.boutin@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Subject: RE: For review / FW: Cryptography topic page

Hi, Chad,

The current version looks fine to me. I would change the order of bullets to Block ciphers, hash functions, PQC, LWC PEC. Since we added block ciphers and hash functions, I think it makes sense to add signature and key establishment, if the list is not too long by adding them. In fact, block ciphers, hash functions, digital signature and key establishment are current the most well deployed 4 crypto tools. PQC, LWC and PEC are "advanced" areas.

By the way, can you explain "continues to lead public and private collaborations"? I think you are more sure about what term to use. By "private collaborations", my understanding is that it implies collaboration with private sectors. Is it correct?

Lily

From: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Sent: Monday, October 25, 2021 3:30 PM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Subject: Re: For review / FW: Cryptography topic page

Yes, the nearly 50 goes to (I think) The brooks act of the 1970s which started this responsibility for us in statute.

From: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Date: Monday, October 25, 2021 at 3:14 PM
To: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>, Chen, Lily (Fed) <lily.chen@nist.gov>, Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Subject: RE: For review / FW: Cryptography topic page

Thanks Matt. I think Ben's question primarily concerns the time period we want to talk about. I'll leave it as "…nearly 50 years" if no one has issues.

CB

From: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Sent: Monday, October 25, 2021 3:10 PM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Subject: Re: For review / FW: Cryptography topic page

For that comment, we still don't want any mention of intelligence. Our scope by law is non-national security systems.

Our work started directly as part of IT/Computer systems and does not pre-date that in non-IT cipher work.

From: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Date: Monday, October 25, 2021 at 3:07 PM
To: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>, Chen, Lily (Fed) <lily.chen@nist.gov>, Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Subject: RE: For review / FW: Cryptography topic page

Will do, Matt. Revised version attached.

If you, Lily or Morrie have thoughts on the one remaining question in the margin, I'll work your answer in.

CB

From: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Sent: Monday, October 25, 2021 3:02 PM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Cc: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Subject: Re: For review / FW: Cryptography topic page

Overall all I think its good and Lily might have inputs to be sure the text is clear.
Drop the last item on Revamping…. . .   I don't want that on the page right now.

From: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Date: Monday, October 25, 2021 at 2:59 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>, Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>, Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Cc: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Subject: RE: For review / FW: Cryptography topic page

Matt, Lily, thanks for your quick input. I have removed some of the bullets and substituted others per your comments.

Please have a look at these revisions and let me know your thoughts about the remaining questions. Feel free to answer in the margin comments … I'll work your answers into the final.

CB

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Monday, October 25, 2021 1:58 PM
To: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>; Boutin, Chad T. (Fed)

<charles.boutin@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Cc: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Subject: RE: For review / FW: Cryptography topic page

Hi, Chad,

I agree with Matt about not including intelligence usage of cryptography. NIST crypto standards, like DES, are public standards and for everyone to use. This is a significant milestone in the cryptography history.

I should have warned you that our annual report put crypto standards and testing all together. That is why in our annual report a lot of content is about texting.

Block cipher and hash function are essential blocks and implemented in almost every IT device. If you need anything about PEC, please let us know.

Lily

From: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Sent: Monday, October 25, 2021 12:59 PM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Cc: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Subject: Re: For review / FW: Cryptography topic page

My .02$ on this.

Lets not mention intelligence at all in this page, that is not our scope for our work and I am not sure how or where encryption gets implemented outside of technology? That comment does not make sense to me.

I would drop all the testing pieces. Drop FIPS 140, CMVP, CAVP.

Add in instead: Privacy Enhancing Cryptograph: https://csrc.nist.gov/Projects/pec
Hash Functions; https://csrc.nist.gov/Projects/Hash-Functions
Block Ciphers: https://csrc.nist.gov/Projects/block-cipher-techniques

Hash and Block are building block items and PQC and PEC are newer and under development.

From: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Date: Monday, October 25, 2021 at 12:49 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>, Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Cc: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>, Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Subject: For review / FW: Cryptography topic page

Matt, Lily, Morrie,

I've put together this draft text that we hope to use to fill out the cryptography topic page. We'd like to get it polished and ready to post by Wednesday morning, as that is the day we are planning to add Matt's interview video that links to the page.

Would you mind having a look sometime today or tomorrow (10/25-26)?

As with our other topic pages, PAO wants to keep the information at a high level and understandable to the layperson. Lily was kind enough to send me to the 2020 Annual Report, so I took the structure and language from it as much as possible. However, my editor still has four questions (see my doc's margin comments) and I'd like to get those addressed with your help.

Thanks in advance, and please let me know if you have questions or concerns.

Best,
CB

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Tuesday, October 19, 2021 3:11 PM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Cc: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Subject: RE: resources? / FW: Cryptography topic page

Hi, Chad,

Let's see if we can find something useful for you. See page 19 of 2020 Cybersecurity and Privacy Annual Report (nist.gov).

Is the information useful? Please let me know.

Lily

From: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Sent: Tuesday, October 19, 2021 2:10 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Cc: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>; Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Subject: resources? / FW: Cryptography topic page

Hi Lily, Morrie,

Up in NIST PAO we're trying to fill out this topic page https://www.nist.gov/cryptography with a brief summary of NIST's cryptography activities and accomplishments. I'm planning to draft it in the next day or so and I wanted to check with you beforehand.

The text I'm writing doesn't need to be very long. It's going to resemble our pages on AI, Climate and Bioscience. Using the same basic structure, I suspect I'll begin with a few sentences on our reasons for pursuing crypto, then a brief second paragraph with our major historical accomplishments. Then I'll put our current efforts into bullet format.

Do you have any resources I could mine? I've got some ideas of course but I don't want to forget anything.

Copying Matt in case he has thoughts.

CB

From: Materese, Robin L. (Fed) <robin.materese@nist.gov>
Sent: Monday, October 18, 2021 4:16 PM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Cc: Huergo, Jennifer L. (Fed) <jennifer.huergo@nist.gov>; Stein, Ben (Fed) <benjamin.stein@nist.gov>
Subject: RE: Cryptography topic page

So the key accomplishments section is likely were some of the "historical" work would go, I imagine.

Generally, the overview section isn't super long. The AI one is a good guide, though I don't know that we'd need to use the accordion functionality for the crypto page. You could take a look at the Climate or Bioscience page, too.

In terms of projects, we can select which 4 project & program pages we want to feature on the page, but they have to be projects & programs that have P&P Drupal pages. That said, I suspect there AREN'T any Drupal P&P pages beside the three already featured there, because when I click on "view all," I get a note that there aren't any… Sigh!

Last, we have the option of adding a Featured Content list at the top right. You can see what's there on the other pages. If you have pages we should link to here, let me know. In this space, it could go to CSRC pages.

Is this at all helpful?

-- Robin

From: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Sent: Monday, October 18, 2021 3:12 PM
To: Materese, Robin L. (Fed) <robin.materese@nist.gov>
Cc: Huergo, Jennifer L. (Fed) <jennifer.huergo@nist.gov>; Stein, Ben (Fed) <benjamin.stein@nist.gov>; Boutin, Chad T. (Fed) <charles.boutin@nist.gov>

Subject: RE: Cryptography topic page

WE FIGHT (you asked for that)

Crypto has a long and storied history 'round here. How far back do we want to go? Do we only want projects we can link to? Ditto stuff PAO has covered?

Also, I'm surprised the page doesn't already have links to other crypto projects like lightweight C, post-quantum C, privacy-enhancing C, etc. and our encryption standards. Perhaps also anything relevant the NCCoE is working on, though that may be beyond our scope here. Generally, is there any way we can find and link to those other pages?

I can whip you up some text, just let me know your thoughts on these Q's for some rough guidelines. And how much text you'd want in terms of word count.

Thankee,
CB

From: Materese, Robin L. (Fed) <robin.materese@nist.gov>
Sent: Friday, October 15, 2021 10:22 AM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Cc: Huergo, Jennifer L. (Fed) <jennifer.huergo@nist.gov>; Stein, Ben (Fed) <benjamin.stein@nist.gov>
Subject: Cryptography topic page
Importance: High

Hi Chad,

For the post-quantum cryptography video (with Matt Scholl) that the video team is working on, we need a page to send people to. I'm thinking we send people here:
https://www.nist.gov/cryptography

But the page is SUPER bare.

Think you can quickly craft me some overview text about our work in cryptography + perhaps some "key accomplishments" so that we can build out the page a bit?

The video and Matt's accompanying Q&A blog post are going up the week of Oct 25… so it's quick turnaround. What say you?

-- Robin