From: Scholl, Matthew A. (Fed)
To: Stine, Kevin M. (Fed)
Subject: Re: some proposed updates to new crypto landing page
Date: Wednesday, October 27, 2021 9:37:56 AM

We certainly can use it for that and can build it out with new items

---

From: Stine, Kevin M. (Fed) <kevin.stine@nist.gov>
Date: Wednesday, October 27, 2021 at 9:34 AM
To: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Subject: Re: some proposed updates to new crypto landing page

> Ok got it. So my thought was the text and links below would be the landing page text for crypto program as a whole (inclusive of the two validation programs and applied crypto at NCCoE). My guess is this would be pretty static content and have content of general "usability" for a broad audience. It would then link to detailed pages for more info.

On: 27 October 2021 09:30,
"Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov> wrote:

So the long story:

When PBA went to clear the video with Jim, he wanted a pointer web site for folks to go to as part of the video and blog. PBA was concerned that the CT Group site was not the same audience and would lose folks. PBA suggested a short landing page that could be cited in the video if folks wanted to "read a bit more."
PBA set it up last week and pulled language from the annual report, ran the first set of language and links by us and then it was edited by Ben Stine.

So the initiation of the page was to help in clarity on the video and not intended as an overall NIST crypto page.
We now have the option to grow it as a NIST page going forward, take it down and relink the video after Nov-ish or do something else.
The page right now is owned and managed by PBA but they will work with us going forward on what we want to do.

From: Stine, Kevin M. (Fed) <kevin.stine@nist.gov>
Date: Wednesday, October 27, 2021 at 9:23 AM
To: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Subject: Re: some proposed updates to new crypto landing page

> The page is supposed to be a landing page for the broad crypto program and not the specific scope of the video, correct? Just trying to understand the purpose of the page and how folks will use it if it doesn't provide some indication of the depth and breadth of our crypto-related work.

On: 27 October 2021 09:20,
"Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov> wrote:

It was a page put together by PAO in a very short time frame as a starter so they can have a simple pointer for the blog post and video going up today.

I specifically did not want CMVP on this page as the starter since the blog and video are not about test or conformance.

There are other items that need to be considered ahead of some of the listing such as mutli party schemes, signature schemes, random numbers etc.
The primary listing of work is here: https://csrc.nist.gov/Groups/Computer-Security-Division/Cryptographic-Technology and this is the main page we currently use.

This highlights some of the problems with having higher level pages, keeping them in synch when they are managed by folks outside the programs while also trying to have pages that are for different audiences that the current crypto sites really don't speak to but we can, and will, update this page going forward.

From: Stine, Kevin M. (Fed) <kevin.stine@nist.gov>
Date: Wednesday, October 27, 2021 at 6:01 AM
To: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Subject: some proposed updates to new crypto landing page

I got a copy of the new crypto page which will also hang off of nist.gov/cybersecurity. https://www.nist.gov/cryptography

The text and content are super narrowly focused and don't give a full picture of NIST's crypto work. With DHS stepping up their messaging around crypto, I think we want to tell a more complete picture of what we do and why it's important.

The page currently doesn't include CMVP or CAVP, and doesn't include the applied crypto work at NCCoE on crypto agility (PQC migrations), CMVP automation, TLS 1.3 visibility, etc. While not directly part of the crypto group, these are definitely part of our crypto program.

Minimally, it should include links to the following in the main page links and to several of these in the Featured Content list of resources.

- Cryptographic Standards and Guidelines
- Post Quantum Cryptography
- Lightweight Cryptography
- Privacy Enhancing Cryptography
- Cryptographic Programs and Laboratory Accreditation
- Cryptographic Module Validation Program (CMVP)
- Cryptographic Algorithm Validation Program (CAVP)
- Applied Cryptography at NCCoE

Would you be ok with text like this below to replace what's currently on the page? This which pulls from what's on the page now as well as adds key public messages from other crypto resources including content developed by the crypto strategic plan group.

Cryptography involves techniques for exchanging secure messages even in the presence of adversaries. As our electronic networks grow increasingly open and interconnected, it is crucial to have cryptographic standards, algorithms and encryption methods that provide a foundation for e-commerce transactions, mobile device conversations and other exchanges of data. NIST has fostered the development of cryptographic techniques and technology for nearly 50 years.

NIST provides trusted tools and resources for the sound use of cryptography.

- *We work with stakeholders around the world to develop strong, trusted cryptographic standards and guidelines. This open process brings together industry, government and academia to develop* ***workable approaches to cryptographic protection that enable practical security.***
- *NIST has cryptographic standards for a variety of IT needs. Since publishing the first Data Encryption Standard for federal systems and financial transactions in the 1970s, our work in cryptography has continually evolved to meet the needs of the changing IT landscape. Today,* ***NIST cryptographic solutions are used in applications from tablets and cellphones to ATMs and top-secret federal data.***
- *NIST helps to design and test cryptographic algorithms used to create virtual locks and keys. We also assist in their use and help to guide how those locks are installed and how effectively they suit the intended purpose.* ***NIST's validation of strong algorithms and implementations builds confidence in cryptography****, increasing its use to protect the privacy and well-being of individuals and businesses in the digital age.*
- *NIST looks to the future to make sure we have the right cryptographic tools ready to protect our digital identities, data, economy, and way of life as new technologies are brought from research into operation. For example, NIST has under way a competition to* ***develop new kinds of cryptography to protect our data when***

***quantum computing becomes a reality**. At the other end of the spectrum, we are advancing so-called **lightweight cryptography** to balance security needs for circuits smaller than were dreamed of just a few years ago.*

...and then include the links above for more information?