From:	Scholl, Matthew (Fed)
To:	Stine, Kevin M. (Fed)
Subject:	Re: update for Walt re PF
Date:	Monday, February 11, 2019 9:29:06 AM
Attachments:	DraftCyrptoTP.docx TPs for Chamber on Wed.docx

Here are some crypto TPs to start with. Also attached is an old Chuck to Chamber TPs that Adam did. I like the format.
We might want to get Adam in on this when Haymen has his first wack?

From: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Date: Friday, February 8, 2019 at 11:49 AM
To: "Stine, Kevin (Fed)" <kevin.stine@nist.gov>
Cc: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Subject: Re: update for Walt re PF

Yes, I will work some up this weekend.

From: "Stine, Kevin (Fed)" <kevin.stine@nist.gov>
Date: Friday, February 8, 2019 at 10:16 AM
To: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Subject: Fw: update for Walt re PF

Do you have core talking points or status points you want Walt to make on Crypto, including FIPS 140-3, etc?

Plan is to have talking points done by next Friday.

From: Mat Heyman (b) (6)
Sent: Friday, February 8, 2019 10:11 AM
To: Stine, Kevin (Fed)
Subject: update for Walt re PF

Kevin,
I'll be starting for real on Walt's talking points later today and this weekend. Please cc me on any updates to Walt on the PF -- along with any of the details you have in mind for the other key items that he should cover, especially:
-Crypto (PQC, and potentially FIPS 140-3 finalization if signed by DOC by then)
- AI
Thanks.

Mat

The integrity of a standard is a direct function of the integrity of the process used to develop it, so NIST takes the transparency, traceability and openness in the development of our standards *very* seriously.

As we look to continuing to provide answers that fundamentally secure technologies to improve our economy, protect our personal information and enable the promises of the future, NIST looks for core capabilities that enable these promises. Once such capability is encryption.

Our long history together working collaboratively and communally in encryption has resulted in a global use and acceptance in cryptography as a foundational security element.

Going to the future, NIST is continuing this work, with this community in an open, transparent and traceable process. Our work in Post Quantum Cryptography continues with the recent announcement of algorithm down selects to 17 Public Key Algorithms and 9 Key Management Schemes that we will continue to evaluate, bench mark and test to ensure that we have new and appropriate cryptography in place prior to the emergence of quantum capabilities.

We are re-designing and rethinking how we conduct testing and conformance for cryptographic products used by the US Government. Putting more responsibility and generation of conformance evidence in the hands of industry. Reducing time to market, reducing cost to maintain compliance and ensuring that the Government has effective and up to date technologies. This is seen in the recently released update to the government testing standard FIPS 140-3 [SHOULD BE OUT BY RSA]

We ask that you continue to work with us, side by side, as we develop new, usable and effective cryptography for the challenges we face in the future.

- Thank You to The Chamber of Commerce for the invitation and the Honor of Speaking at the Cyber Security Summit.

- **THANK / RECOGNIZE ANY SPECIAL GUESTS IF APPROPRIATE.**

- **Introduce Yourself**

  I am Chuck Romine of the Information Technology Lab at the National Institute of Standards and Technology. We are a metrology agency in the department of commerce with a diverse and important mission of providing base measures and metrics that advance US industry and improve our quality of life.

- **Introduce NIST**

  Depending on your context you might know NIST as the keeper of the atomic clock, the source of all US calibration standards, the US Science Agency who led the World Trade Center Building Collapse Study or perhaps for our work in cybersecurity.

  Since early times in cybersecurity, it was part of NISTs mission. This is due to the United States early and fundamental realization that this is not just a security issue or a National Security concern. Cybersecurity is an economic and business issue.

  As we continue to address this issues for the government and for the nation, we are currently finishing up the last Fiscal Year and spent some time to reflect on the events of FY 14. It was a busy year in cybersecurity from Breaches, Vulnerabilities, Data Thefts and the Constant talk of Advanced Persistent Threats.

- **Talk About Cybersecruity Issue as a Business Issue**

  Now more than ever the understanding and the context of economic and commerce issues with the business reliance on IT are critical for getting cybersecurity right.

  NIST works diligently and collaboratively to ensure that balance, effective communication, usability of our products and common sense are consistently applied in the cybersecurity recommendations we make and that guidance and implementations support and promote business.

  It has been a busy year for all of us and, the public discourse on cybersecurity and the focus on the issue are a good sign of our collective work to continue to address this shared issue. We are seeing a positive trend to looking at the threats and what we need to do to counter them. Lessons learned, open dialogue and cybersecurity information sharing are important for all of us and focus on Risk rather than victims is one of the many things making that happen.

Commented [MS1]: Up To You If You Want to Include This. Intent is to shift from Blaming Victims of Cybercrime for the criminal act and looking to what can be learned and shared to not allow it to repeat.

The threats we face are not just threats to the USG, as we all know. This last year showed that the business community is a target. Threats seek to exploit and steal assets, intellectual property and personally identifiable information from all of us.

- **Talk About What We Have Done About The Issue**

This last year NIST worked in several areas to address cybersecurity challenges facing the nation.

We worked with industry in an aggressive and active public-private partnership as part of our responsibility in the Presidents Executive Order 13636; Reducing Cybersecurity Risk to US Critical Infrastructure.

In that collaborative effort we, together, created a cybersecurity framework creating a common understanding of cybersecurity that can be expressed inside organizations and externally to suppliers and customers as well. It can be used to create a cybersecurity program, look at existing programs for effectiveness and efficiencies and allow all of us to have this critical dialogue in a common language.

We continued our outstanding work in encryption technologies, providing a set of tools for a trust foundation that we call all build upon. We extended our processes of transparency, trust and traceability in our cryptographic work to ensure full openness and understanding of the source of all our science, decisions and provenience of materials. This is critical for operating in global market where interoperability and security must work hand in hand.

We look to the challenges in the future that we all face, to ensure that the technologies you, as businesses bring to improve our economy and quality of life can be adopted and used safely, securely and with confidence.

These range from the continued work in mobility, cloud computing, social media, connectivity, privacy, usable security, data analytics, security automation and a range of other research and development areas.

We are in the starting phase of our applied engineering center, the newly formed FFRDC, the National Cybersecurity Center of Excellence. Here we bring in communities and stakeholders who have real world, immediate challenges in cybersecurity and construct architectures with industry to show references, using existing technologies, that can meet those challenges.

We continue our work in areas of identity management, internet of things, and the future of IT and communications in an automated and always connected world of the near future.

- **The Ask: Collaboration and Continued Communication**

None of this can be done without your direct help. It is though collaboration with academia, international organizations and most importantly, businesses that we understand the key areas where we can help.

That feedback and collaboration ensures we stay focused and provide technology, tools, and reference that are effective and balanced with the need of business while addressing the cybersecurity threats and vulnerabilities we all face.

Our goal is not to duplicate, but enhance technology development. We do not want to become isolated with cybersecurity requirements but open business with industry led, consensus based international standards participation.

- **Close**

I hope that collaboration and discourse continues with this summit and goes on well into the future.

Thank you all, keep the discourse and discussion going and we look forward to FY 15 and the challenges it brings