NIST Post-Quantum Cryptography Standardization and NSM 10

National Foundation – NSM 10

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

- Maintain the Nation’s competitive advantage in quantum information science (QIS), while mitigating the risks of quantum computers to the Nation’s cyber, economic, and national security.

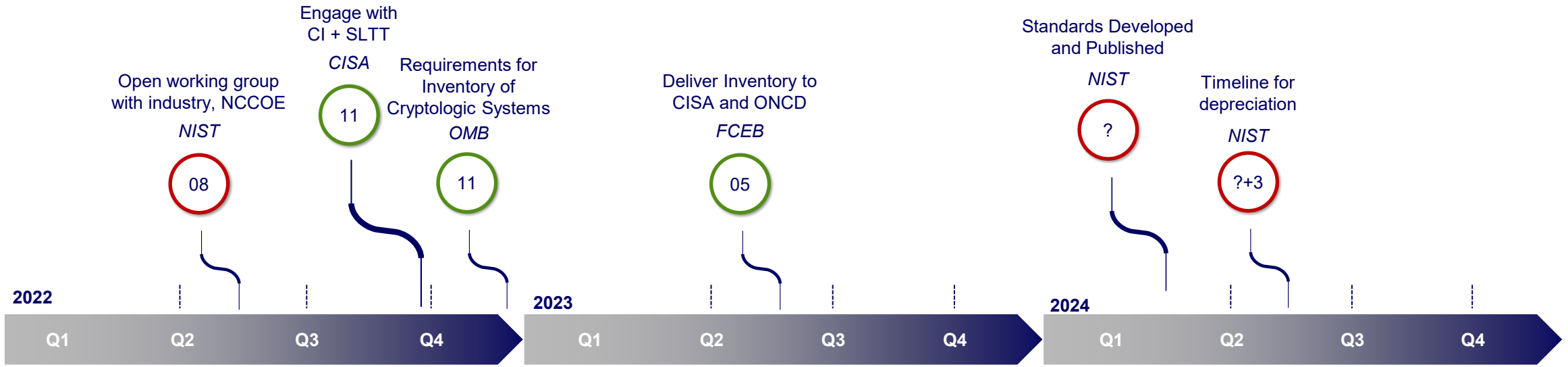
Threat

A quantum computer of sufficient size and sophistication — also known as a cryptanalytically relevant quantum computer (CRQC) — threatens the security of asymmetric cryptography.

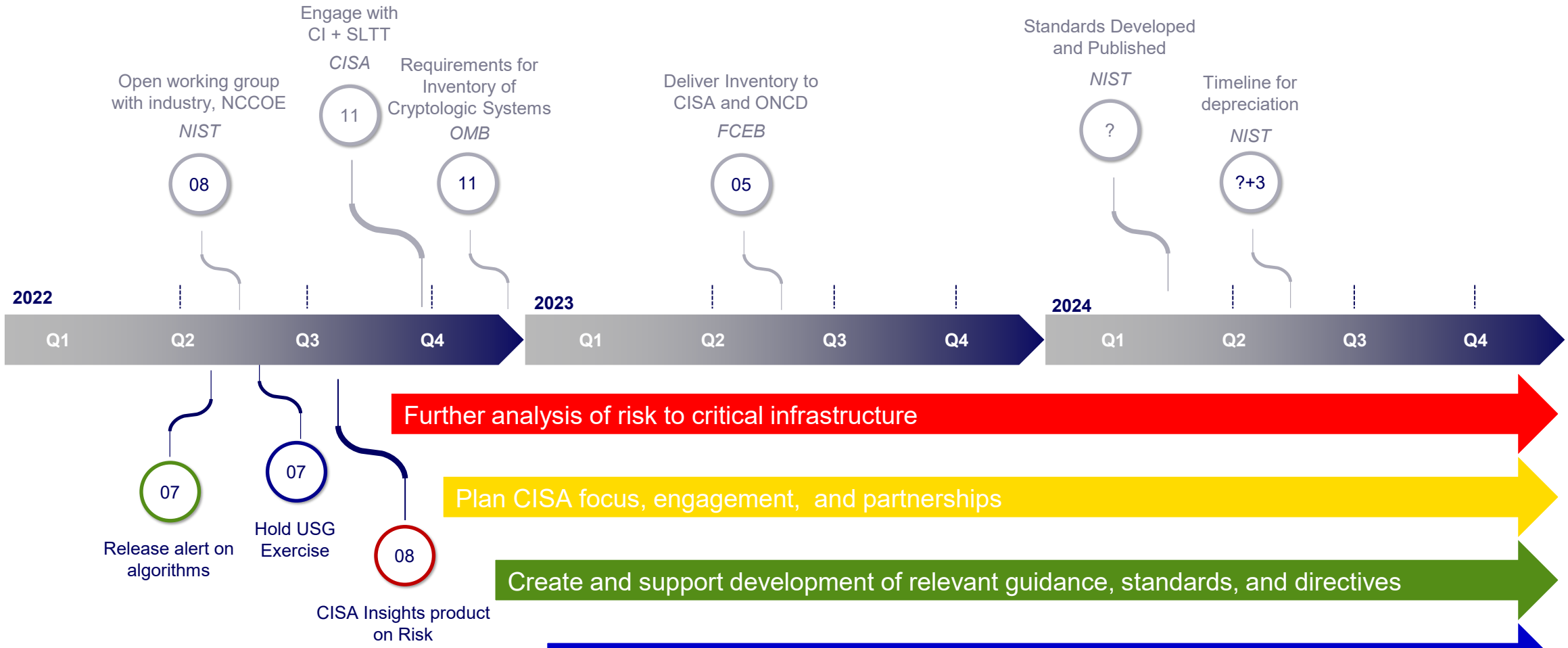
Although the exact timing for the arrival of such a computer is not known, the threat to information protected by asymmetric cryptography exists now because an adversary can collect currently encrypted data and break it when sufficient quantum computation becomes available.

Asymmetric cryptography, or cryptography that uses both public and private keys, is ubiquitous throughout the Federal government, State, local, tribal, and territorial governments (SLTT), and U.S. critical infrastructure.

NSM Timeline

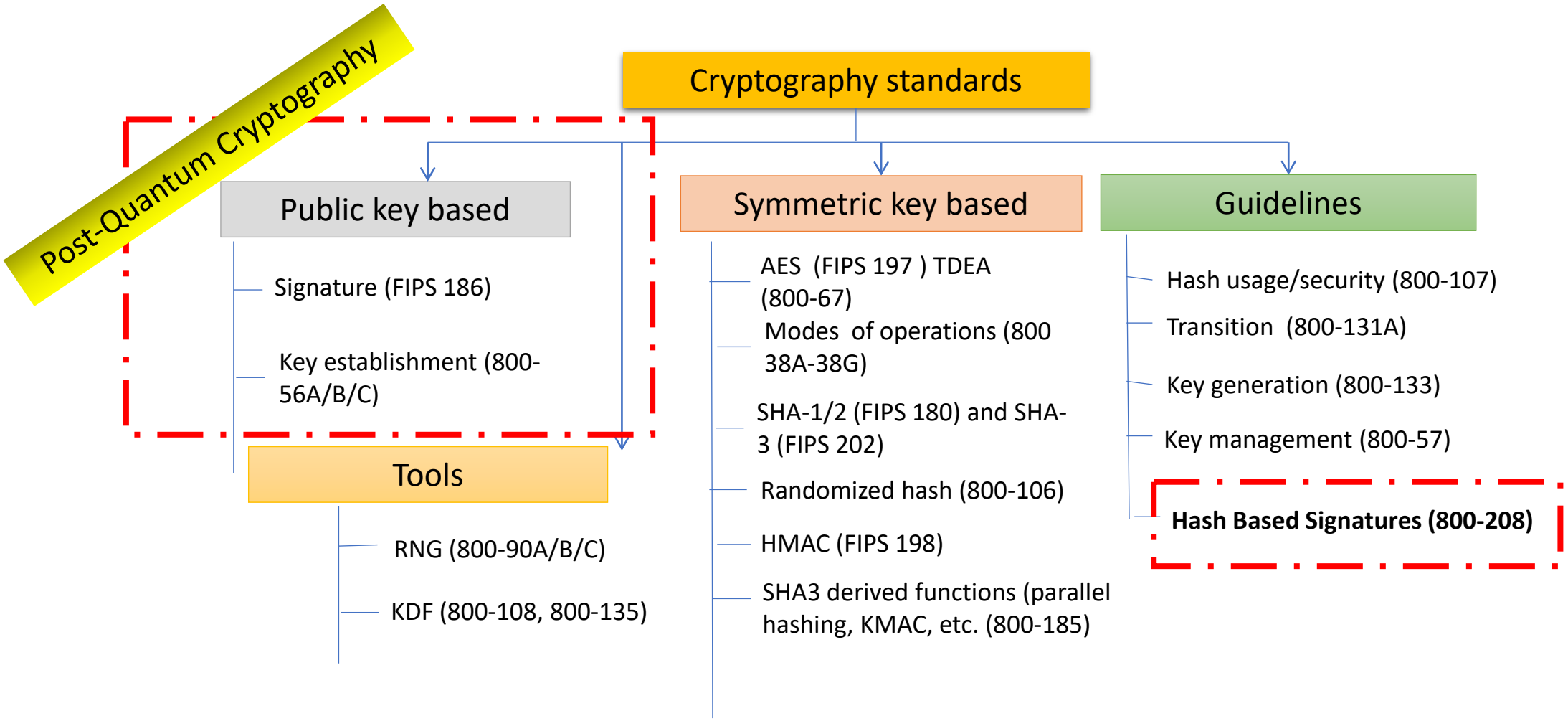


CISA Actions



5

NIST Crypto Standards – PQC Scope



NIST PQC Standards – Milestones and Timeline

2016 Criteria and requirements and call for proposals

2017 Received 82 submissions and announced 69 1st round candidates

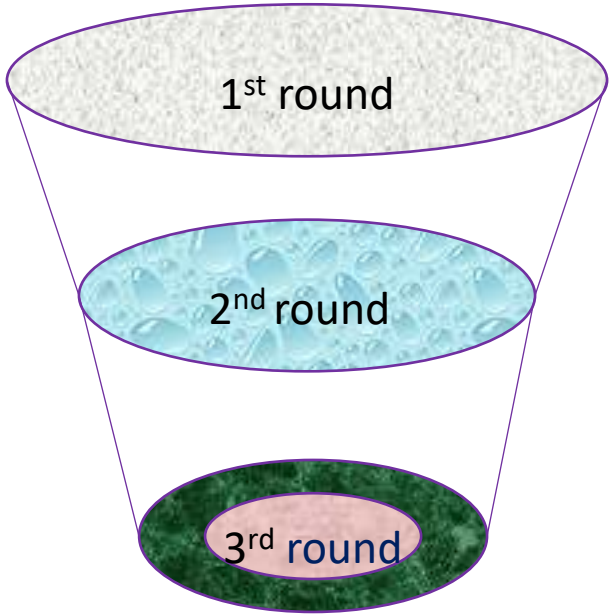
2018 The 1st NIST PQC standardization Conference

2019
Announced 26 2nd round candidates

The 2nd NIST PQC Standardization Conference

2020 Announced 3rd round 7 finalists and 8 alternate candidate

2021
The 3rd NIST PQC Standardization Conference



SELECTIONS ANNOUNCED July 5th, 2022

2022-2023 Release draft standards and call for public comments

2024 Publish PQC Standards

What Was Selected First

NIST recommend two primary algorithms to be implemented for most use cases:

- CRYSTALS-KYBER (key-establishment) and,
- CRYSTALS-Dilithium (digital signatures). In addition,

- Signature schemes FALCON and SPHINCS+ will also be standardized.

- CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance. NIST expects them to work well in most applications.

- FALCON will also be standardized by NIST, there may be use cases for which CRYSTALS-Dilithium signatures are too large.

- SPHINCS+ will also be standardized to avoid relying only on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

What Is Next

- NIST will create new draft standards for the algorithms to be standardized,
- NIST will seek input on specific parameter sets to include, particularly for security category 1.
- The standards will be posted for public comment, revise the draft standards as appropriate based on the feedback received, conduct final review, approval, and promulgation process will then follow.

- Work with the NCCoE in the Migration To Post Quantum Cryptography Project.

NCCoE Problem Statement

- Migration to post-quantum cryptography (PQC) poses challenges for developers, supply chains, and user organizations.
- A first step in migration is discovery of where and how public-key cryptography is used in the organization's infrastructures, services, and end-user devices and applications (sometimes not immediately obvious).
- Then, the organization can develop a playbook for risk-based acquisition and implementation of quantum-resistant cryptography.

NCCoE Project Goals

Development of tools and approaches to facilitate migration to PQC.

- Demonstrate automated discovery tools to identify instances of quantum vulnerable public-key algorithm use: where, how, and for what they are used – and with what constraints.
- Develop and demonstrate a risk-based approach to prioritizing migration use cases and activities.
- Identify systematic approaches to conducting migration activities (e.g., protocol/product development, developing test/acceptance criteria, distribution and acquisition, integration and implementation, and operation and maintenance.

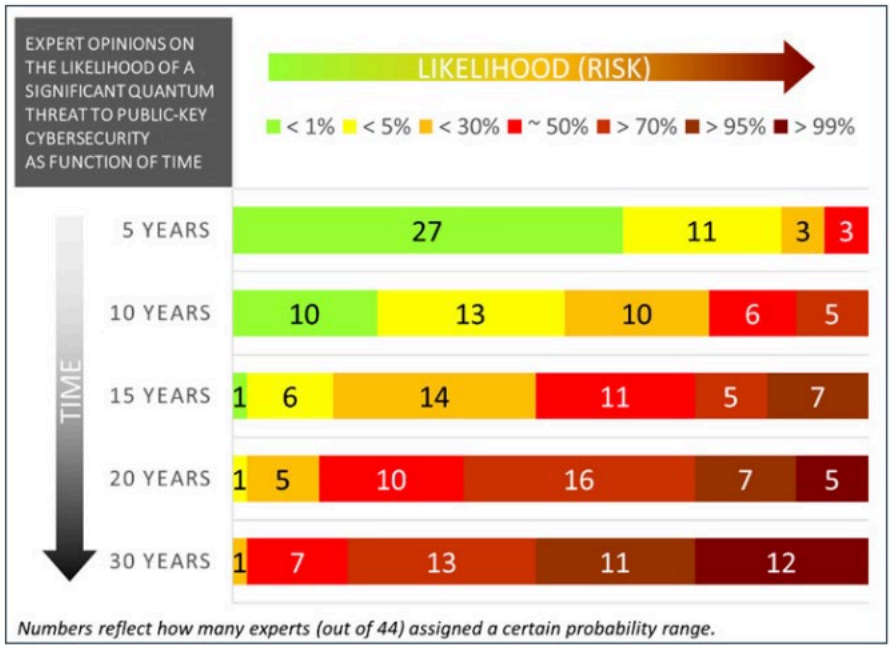
Proposed Timeline for Deprecation?

- NSM States;
- “Within 90 days of the release of the first set of NIST standards… NIST shall release a proposed timeline for the deprecation of the quantum vulnerable cryptography in standards”
- “To mitigate this risk, the US must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, *with the goal of mitigating as much of the quantum risk as is feasible by 2035.*”

  - What is the right information we need to set this date?
  - What are the right questions to ask?
  - Who are the right people to engage?

  - Is this just DH and RSA or should we also transition AES Key size?

OK, so when exactly ? ? ? ?



Source: M. Mosca, M. Piani, Quantum Threat Timeline Report, 2020
available at: https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/