Shielding Secrets:

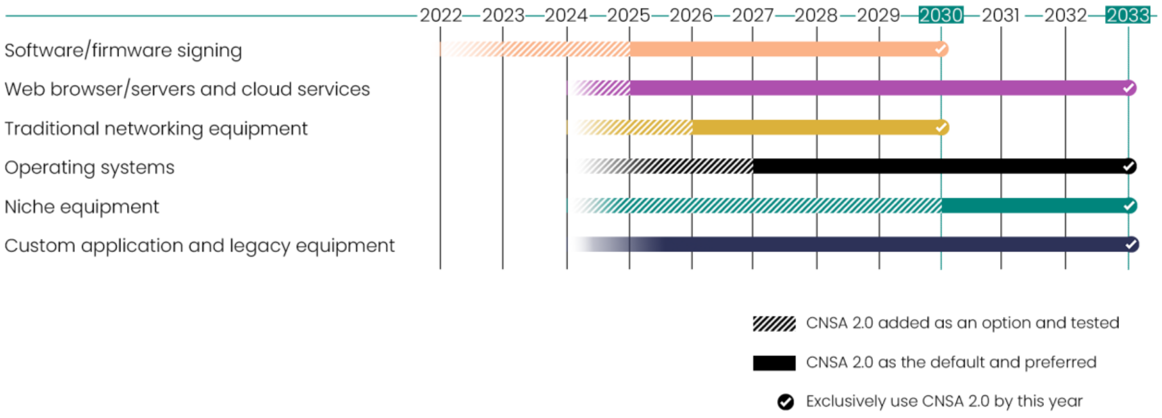
Fortifying Government and Military Data Today with Secure, Cost-Effective, Quantum-Safe Solutions

Roberta Faux, US Head of Cryptography and US Field CTO, Arqit

July 2023

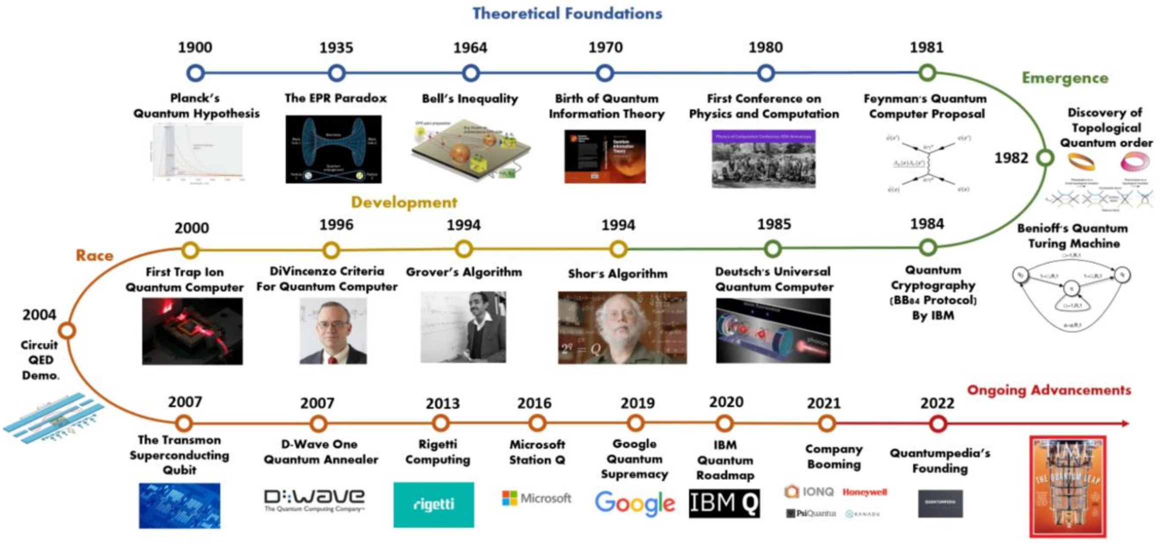
The Commercial Solutions for Classified (CSfC) program was established by NSA, in 2010. This program allows the United States Government and military entities to take advantage of cutting-edge innovations, and access affordable commercial technologies, while maintaining the necessary stringent security standards. Prior to the CSfC program, US Government Agencies relied primarily on specialized, and often expensive solutions, to secure classified information. Advancements in commercial cybersecurity technologies such as quantum-safe solutions, present an opportunity to leverage trusted off-the-shelf products with cost benefits.

CNSA 2.0 Timeline



At the annual CSfC Conference in May 2023, NSA representatives shared the spy agency's perspective on planning, preparing, and budgeting, to transition to quantum-resistant algorithms. This is outlined in CNSA 2.0 which informs National Security Systems (NSS) on algorithms to safeguard from the emerging threat from quantum computers. CNSA 2.0 was provided in accordance with authorities detailed in NSD-42, NSM-8, NSM-10, CNSSP 11, and CNSSP 15. NSA Technical Director for Cryptographic Solutions, William Layton presented an overview on *'Post-Quantum CSfC'*. The message was simple: ***the time is now, and the immediate, currently available solution is to add in pre-shared keys.***

This urgency is driven by the fact that in the future, large-scale quantum computers will crack today's public key encryption, putting at risk the security and integrity of information in our government and military operations. Breakthroughs in quantum computing are increasing at an unanticipated rate, bringing the horizon of the quantum era ever closer. Simultaneously, this means the quantum threat looms over the security of our digital data. It is imperative to adopt quantum-safe solutions to protect our nation's classified data throughout government and military systems.


Theoretical Foundations
1900
Planck's Quantum Hypothesis
1935
The EPR Paradox
1964
Bell's Inequality
1970
Birth of Quantum Information Theory
1980
First Conference on Physics and Computation
1981
Feynman's Quantum Computer Proposal
Emergence
1982
Discovery of Topological Quantum order
Benioff's Quantum Turing Machine
1984
Quantum Cryptography (BB84 Protocol) By IBM
1985
Deutsch's Universal Quantum Computer
1994
Shor's Algorithm
1994
Grover's Algorithm
1996
DiVincenzo Criteria For Quantum Computer
2000
First Trap Ion Quantum Computer
Development
Race
2004
Circuit QED Demo.
2007
The Transmon Superconducting Qubit
2007
D-Wave One Quantum Annealer
2013
Rigetti Computing
2016
Microsoft Station Q
2019
Google Quantum Supremacy
2020
IBM Quantum Roadmap
2021
Company Booming
2022
Quantumpedia's Founding
Ongoing Advancements
D-Wave
rigetti
Microsoft
Google
IBM Q
IONQ
Honeywell
PsiQuantum
XANADU

A Brief History of Quantum Computing (Copyright: Quantumpedia)

Why is NSA recommending pre-shared keys? Pre-shared key for symmetric key agreement is often an overlooked solution to quantum-resistance. Yet, this approach offers many advantages over traditional public key schemes:

- *Rapid migration time*
- *Hyper-scalability*
- *Crypto-agility to support evolution of algorithms*
- *Low implementation complexity*
- *Low latency*
- *Ease of key management*

NSA's publication on 'Quantum Computing and Post-Quantum Cryptography' recommends that some CSfC solutions "*be implemented using symmetric, pre-shared keys that protect against the long- term quantum computing threat.*" Further, "*NSA considers the use of pre-shared symmetric keys in a standards-compliant fashion to be a better near-term post-quantum solution than* *implementation of experimental post-quantum asymmetric algorithms."* There are a growing number of solutions that already strongly align with CSfC's Symmetric Key Management Requirements Annex V2.0, and can help organizations build secure systems tailored to their specific needs.

Symmetric Key Agreement (SKA) allows organizations TODAY to meet with President Biden's National Security Memorandum, NSM-10. NSM-10 outlines the promotion of both the United States leadership in quantum computing and refresh requirements for cryptographic modernization.

Symmetric key agreement solutions meet the stringent security requirements consistent with CSfC programs and can play a significant role in facilitating the adoption of quantum-safe cybersecurity solutions. This is transforming the cryptographic modernization of information security and will enable US Government customers to leverage the latest commercial technology solutions, to achieve nation security mission objectives.