IBM Quantum Safe

Prepare now to understand the impact and risks of quantum

Terrence Head
Business Development Executive of IBM Quantum Safe Team
IBM Quantum
Terrence.Head@ibm.com
202-531-0555

Our mission

Bring useful quantum computing to the world

Make the world quantum safe

Our digital world depends on cryptography, which is used in trillions of transactions on billions of devices

Internet

- Domain name system (DNS)
- Hypertext transfer protocol (HTTP)
- File transfer protocol (FTP)

Digital signatures

- Electronic identification and trust services (eIDAS)
- PDF advanced electronic signature (PAdES)
- Advanced electronic signatures

Critical infrastructure

- Code updates
- Control systems
- Car systems

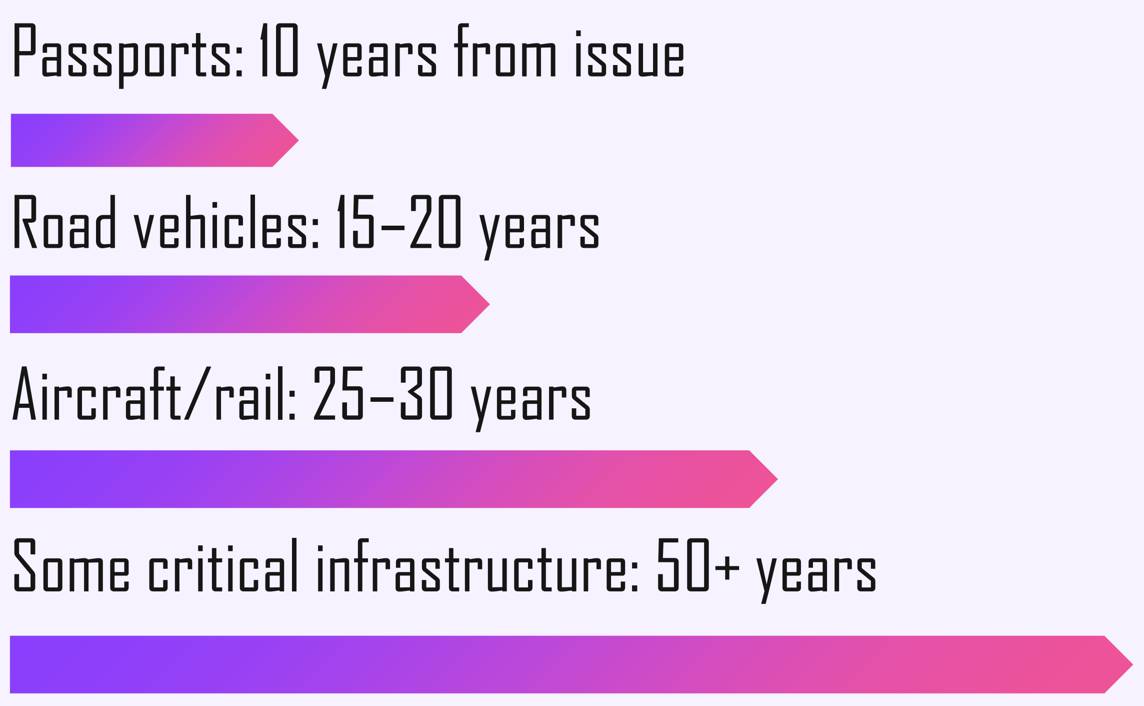
Financial systems

- Payment systems

Enterprise

- Email
- Identity management
- LDAP
- PKI services
- Bespoke applications

Documents that needs to stay secure for a long period of time



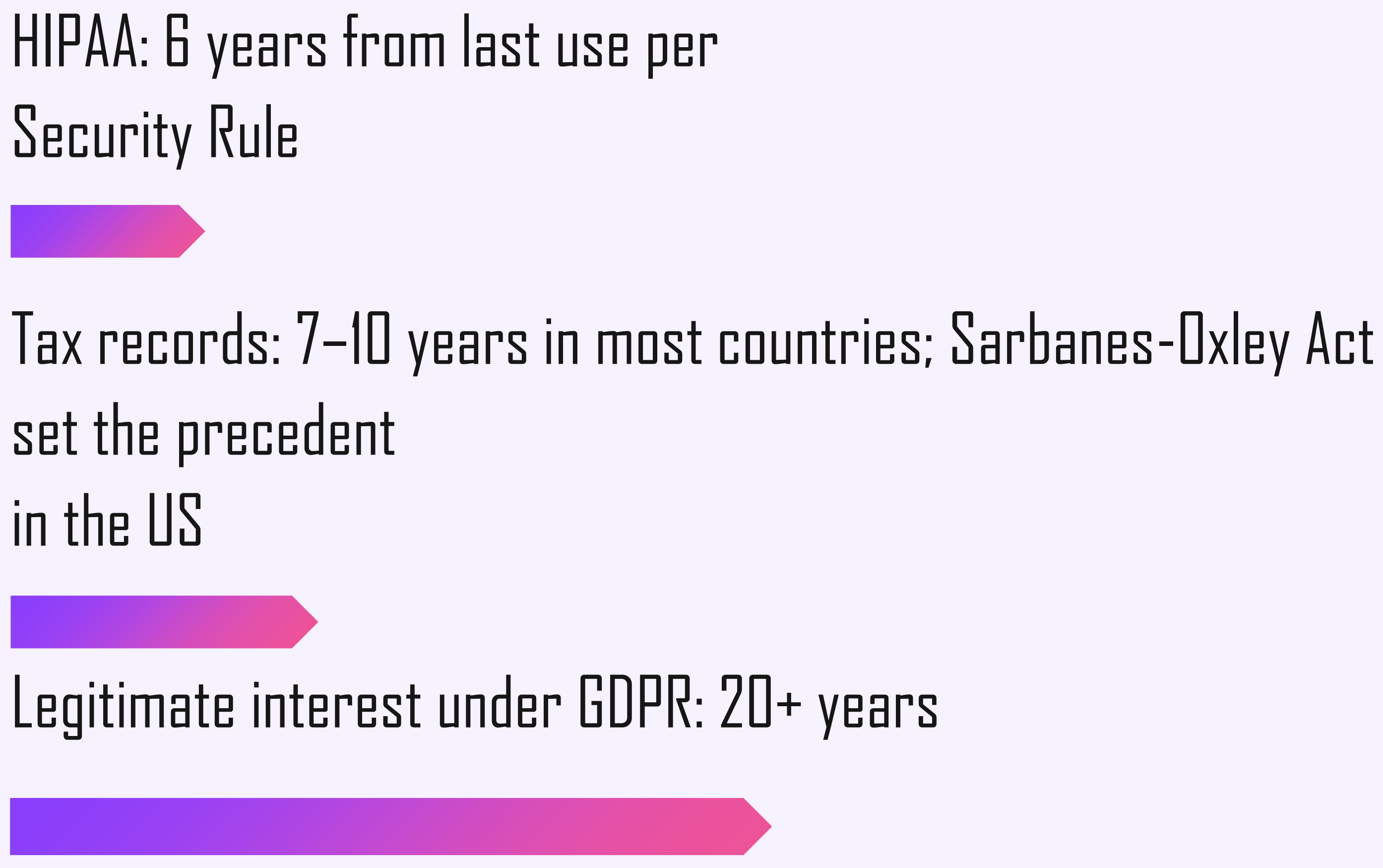
Passports: 10 years from issue

Road vehicles: 15–20 years

Aircraft/rail: 25–30 years

Some critical infrastructure: 50+ years

Data needs to stay secure for a long time



HIPAA: 6 years from last use per Security Rule

Tax records: 7–10 years in most countries; Sarbanes-Oxley Act set the precedent in the US

Legitimate interest under GDPR: 20+ years

Much of today's cryptography relies on hard mathematical problems

Public key encryption

Digital signatures

Key exchange algorithms

RSA

DSA

ECC

ECDSA

DH

Factorization

Challenge: Find prime factors

2322787564435549164834361443028149612994031684727417263786290430508218092253250735821796492729239678595328547390282873154900644025641142681088687405784417436736582322860438955979270980594463654064631679 [illegible] 159001223364261 [illegible] 7126686305773 [illegible] 586434995088 [illegible] 1411035194072 [illegible] 0993984688031458567407248316849706228039701945884045222985355457804905221526364397187245486217526051159916514049067262683351832309929798930626982884352880228081343661786676287332222814070049377025100824571915521143930659330865829303735221526

RSA-2048

= pxq

Difficulty

The most powerful computer today **would take millions of years to find the solution**

Shor's quantum algorithm is anticipated to possibly break RSA in **hours** using hardware available soon.

What are cybercriminals doing now?

Harvest now, decrypt later

Now

Availability of "cryptographically relevant" quantum computers

Later

Harvest confidential data to decrypt later

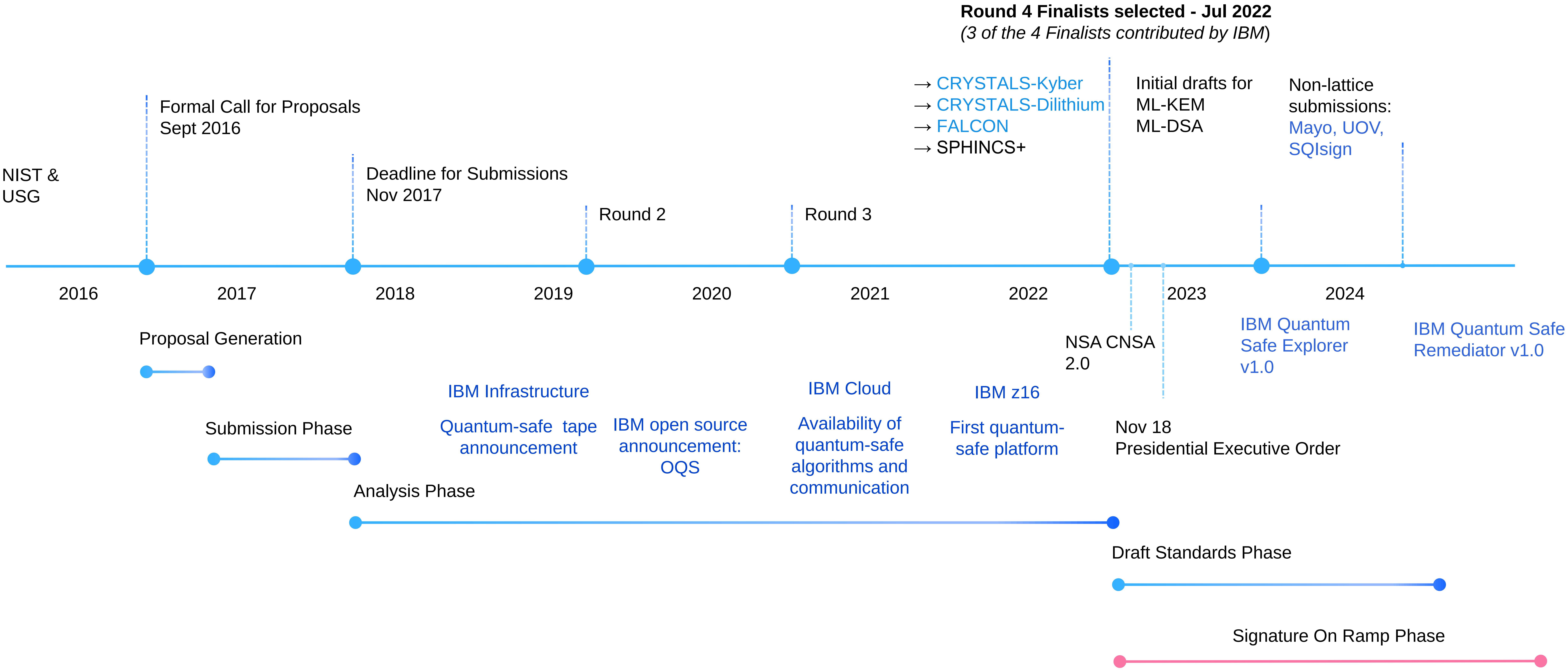
Decrypt lost or harvested confidential data by breaking encryption

Disrupt business with manipulation through fraudulent authentication

Manipulate digitally signed contracts and legal history by forging digital signatures

Quantum Safe Cryptography

NIST Standardization for Quantum Safe Cryptography



Round 4 Finalists selected - Jul 2022
(3 of the 4 Finalists contributed by IBM)

→ CRYSTALS-Kyber
→ CRYSTALS-Dilithium
→ FALCON
→ SPHINCS+

NIST &
USG

Formal Call for Proposals
Sept 2016

Deadline for Submissions
Nov 2017

Round 2

Round 3

Initial drafts for
ML-KEM
ML-DSA

Non-lattice
submissions:
Mayo, UOV,
SQIsign

Proposal Generation

Submission Phase

IBM Infrastructure

Quantum-safe tape announcement

IBM open source announcement: OQS

IBM Cloud

Availability of quantum-safe algorithms and communication

IBM z16

First quantum-safe platform

NSA CNSA
2.0

Nov 18
Presidential Executive Order

IBM Quantum Safe Explorer v1.0

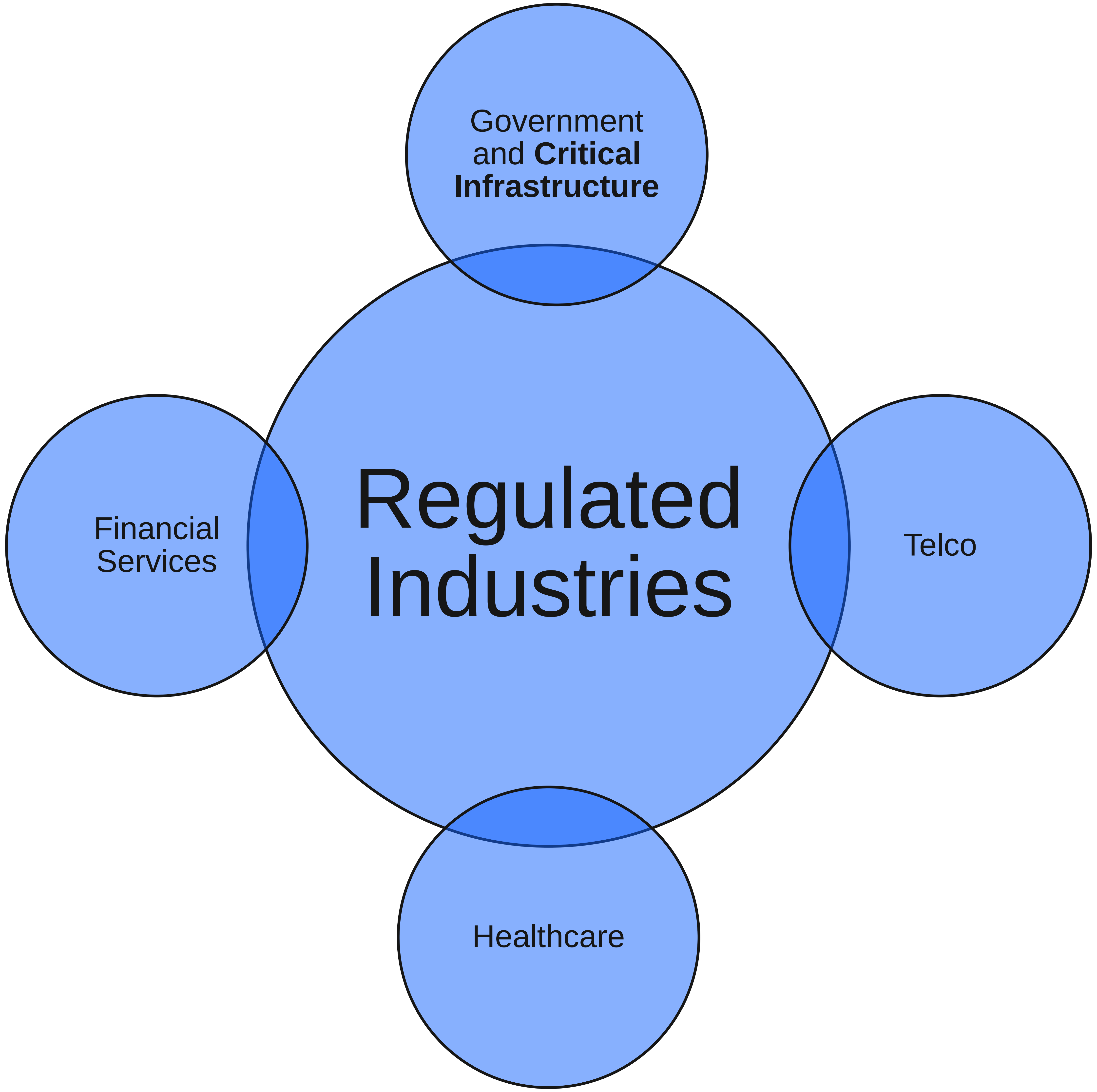
IBM Quantum Safe Remediator v1.0

Analysis Phase

Draft Standards Phase

Signature On Ramp Phase

Who should focus on Quantum Safe Initiative



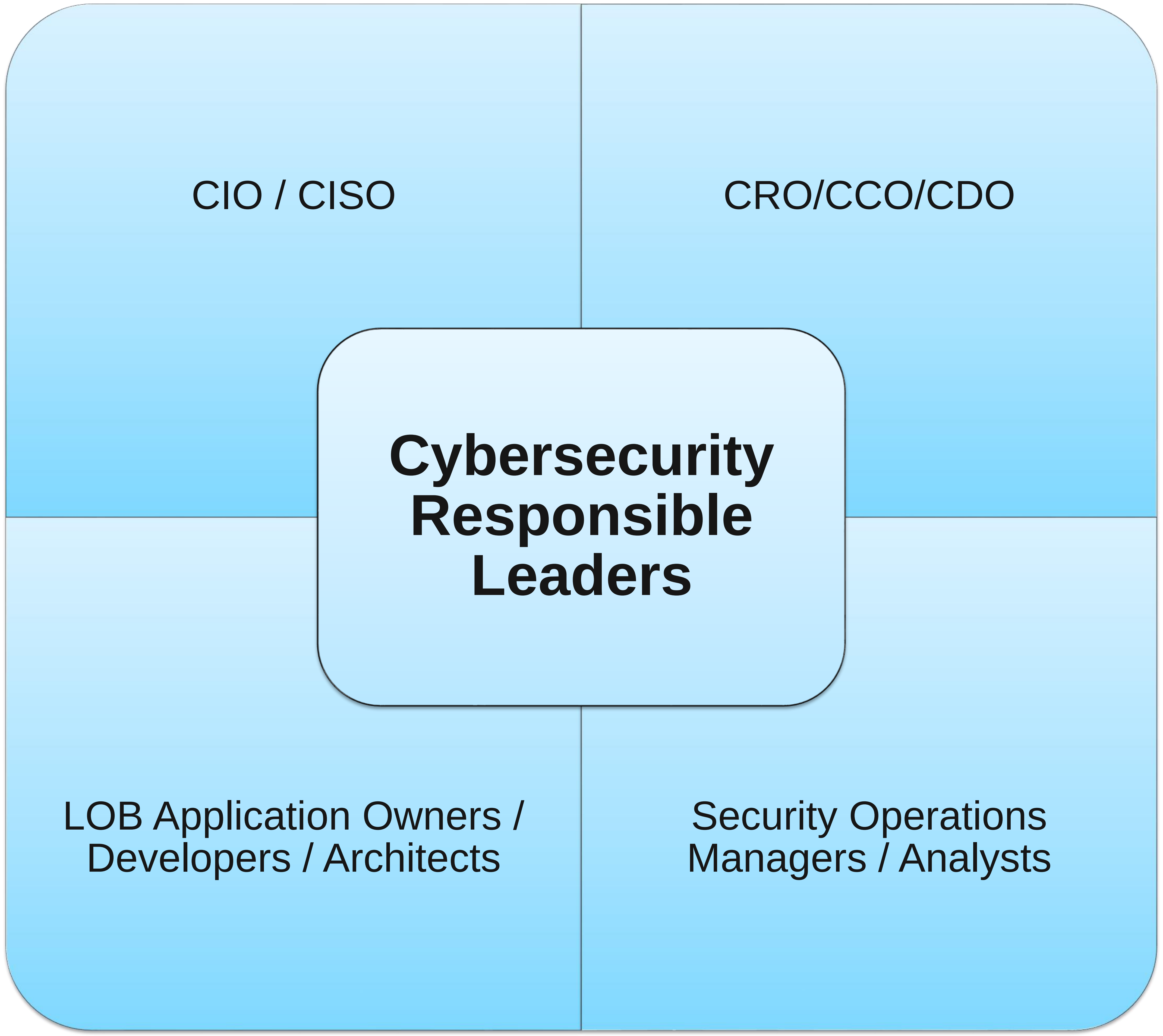
Government and **Critical Infrastructure**

Financial Services

Regulated Industries

Telco

Healthcare



CIO / CISO

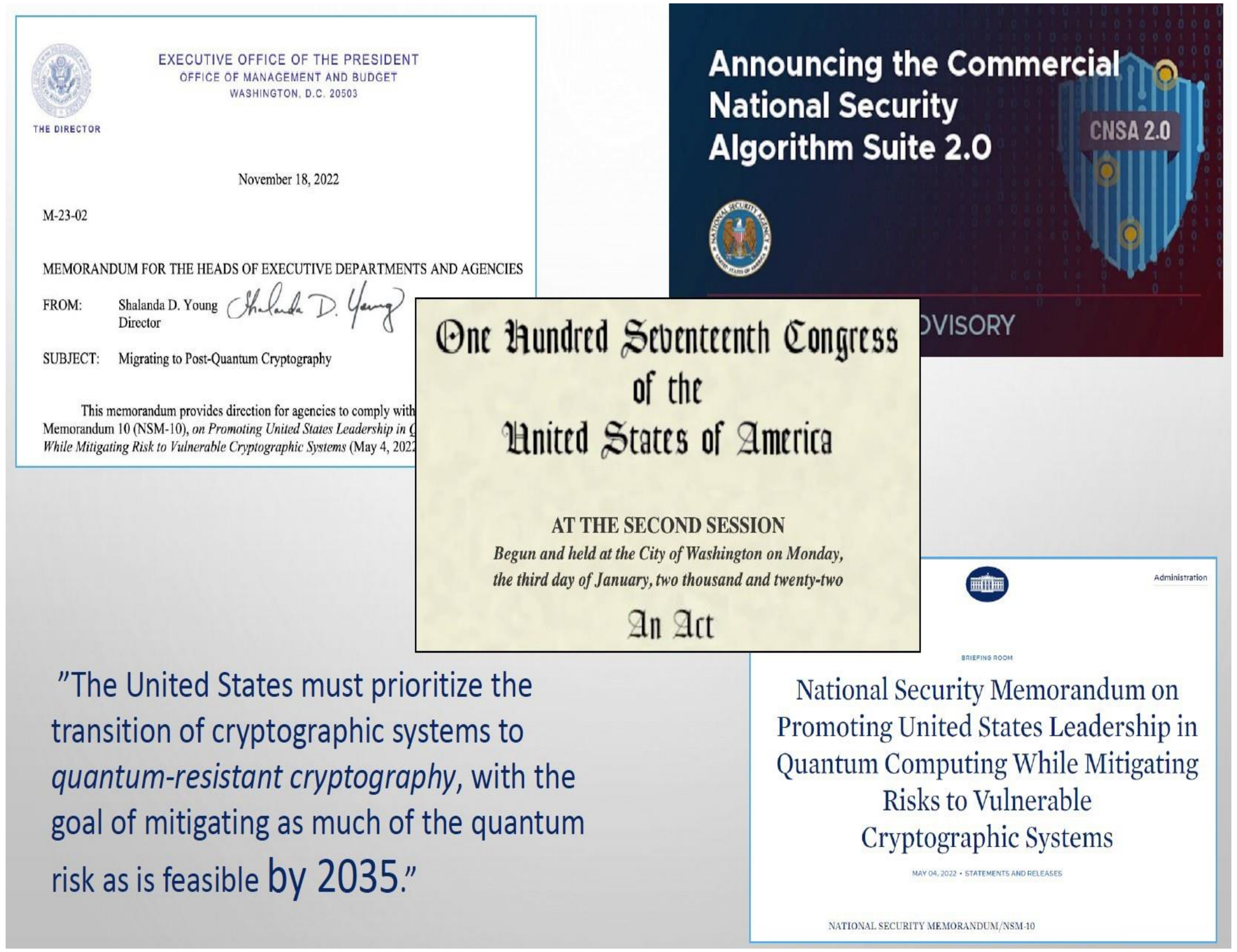
CRO/CCO/CDO

Cybersecurity Responsible Leaders

LOB Application Owners / Developers / Architects

Security Operations Managers / Analysts

US Government Mandates Quantum Safe for Federal Agencies



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

This memorandum provides direction for agencies to comply with
Memorandum 10 (NSM-10), *on Promoting United States Leadership in Q*
While Mitigating Risk to Vulnerable Cryptographic Systems (May 4, 2022

Announcing the Commercial National Security Algorithm Suite 2.0

CNSA 2.0

DVISORY

One Hundred Seventeenth Congress
of the
United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Monday,
the third day of January, two thousand and twenty-two

An Act

Administration

BRIEFING ROOM

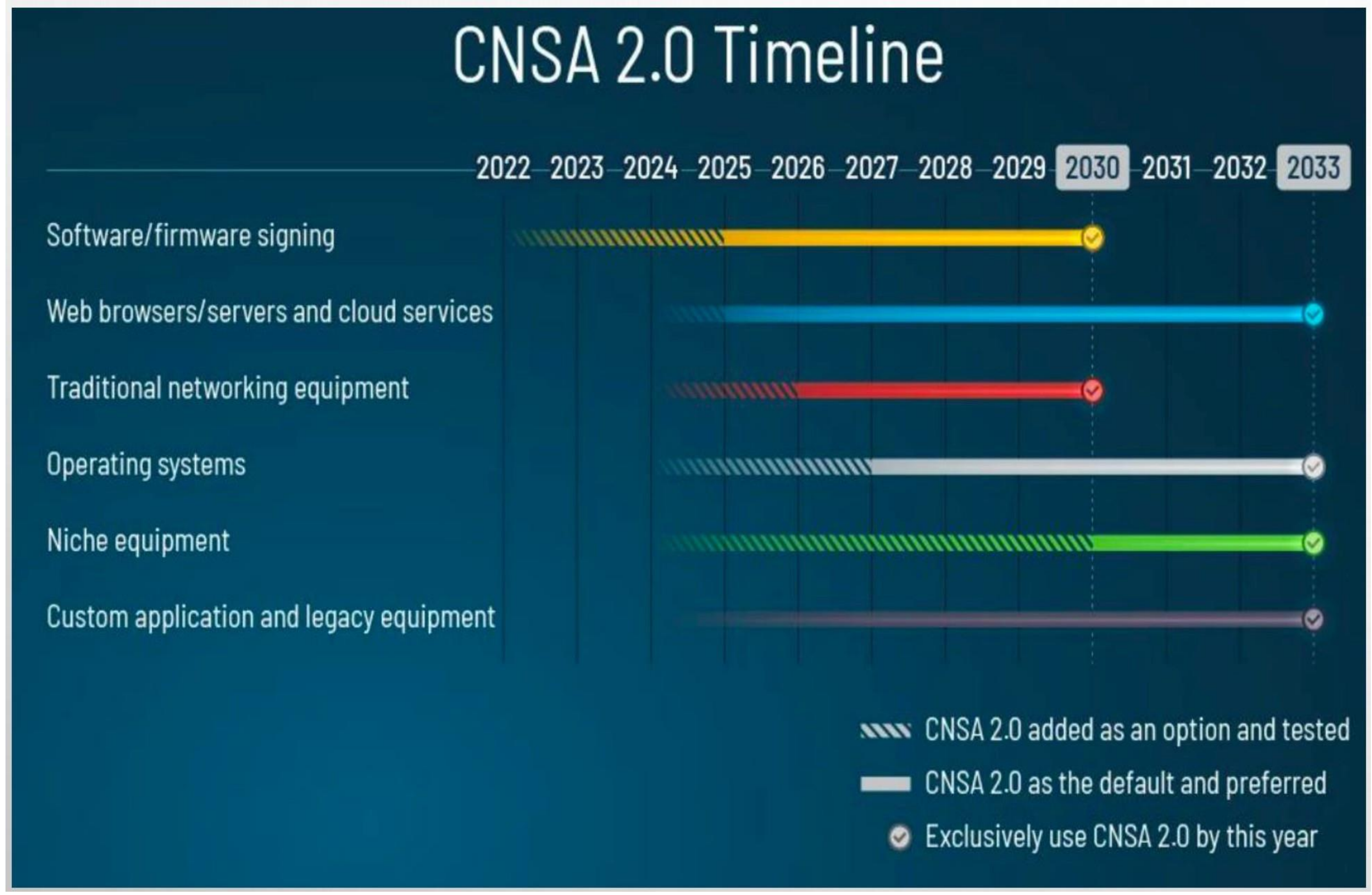
National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

”The United States must prioritize the transition of cryptographic systems to *quantum-resistant cryptography*, with the goal of mitigating as much of the quantum risk as is feasible by 2035.”

CNSA 2.0: Quantum-safe standards are preferred for national security systems by the mid-2020s and required by the early 2030s to defend against threats.



CNSA 2.0 Timeline
Software/firmware signing
Web browsers/servers and cloud services
Traditional networking equipment
Operating systems
Niche equipment
Custom application and legacy equipment
CNSA 2.0 added as an option and tested
CNSA 2.0 as the default and preferred
Exclusively use CNSA 2.0 by this year