NSA CYBERSECURITY

CNSA 2.0 and the Future of Security

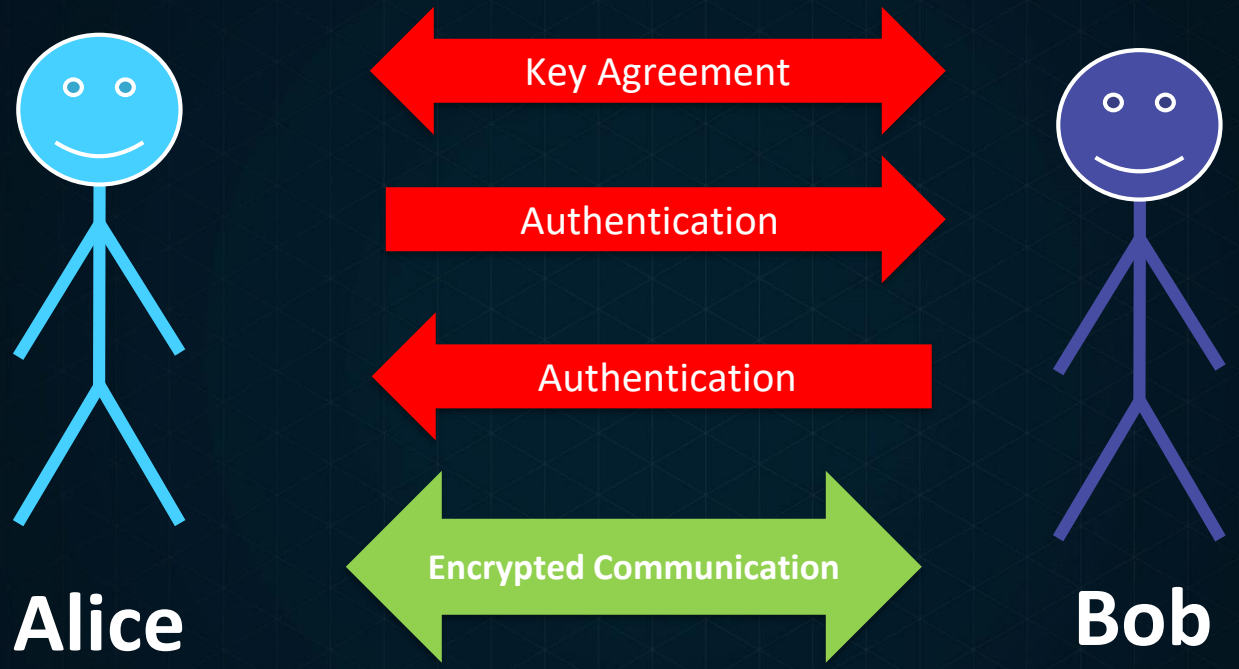
MORGAN STERN, PHD

DECEMBER 4, 2023

Quantum computing

- A new method of computation based on properties of the some of the smallest systems studied in modern physics, such as single photons or electrons.
- Capable of performing very specific types of calculations exponentially faster than classical computers, including:
  - Physics simulations
  - Chemistry simulations
  - The hard problems underlying the most commonly used key distribution and digital signature algorithms
- While currently there are several quantum computers available for use, and there is great promise in the contributions to science and engineering as the field develops further, they have not yet scaled to be cryptographically relevant.

Cybersecurity ramifications of quantum computing



Red algorithms are currently quantum vulnerable. Any vulnerable algorithm can compromise security.

National Security Memo 10

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

3 [T]he United States 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.

3.c.vii Within 90 days of the release of the first set of NIST standards for quantum-resistant cryptography… NIST, shall release a proposed timeline for the deprecation of quantum-vulnerable cryptography… with the goal of moving the maximum number of systems off… within a decade of the publication of the initial… standards.

3.c.ix Until the release of… of NIST standards… FCEB Agencies shall not procure any commercial quantum-resistant cryptographic solutions for use in IT systems supporting enterprise and mission operations.

3.c.x Within 1 year… the Director of NSA… shall provide guidance on quantum-resistant cryptography migration, implementation, and oversight for NSS.

With these goals in mind, NSA released the Commercial National Security Algorithm (CNSA) 2.0 Suite September 2022 (https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/)

Commercial National Security Algorithm (CNSA) 2.0 Suite

Algorithm	CNSA 1.0	CNSA 2.0	Relevant NIST standards
Block Cipher	AES-256	AES-256	FIPS 197
Cryptographic Hash	SHA-384	SHA-384 or SHA-512	FIPS 180-4
Public Key Establishment	RSA-3096 or ECDH P-384	ML-KEM-1024 (aka Kyber Level V)	FIPS 203
Digital Signature (all use cases)	RSA-3096 or ECDSA P-384	ML-DSA-87 (aka Dilithium Level V)	FIPS 204
Software/Firmware Signature	RSA-3096 or ECDH P-384	LMS or XMSS (LMS 256-192 recommended)	SP 800-208

NSA will update protection profiles as industry develops appropriate standards because product lines may develop at different speeds. CNSA 1.0 algorithms will continue to be used until solutions can operate with CNSA 2.0.

Brief notes from Quantum Information Science: Why CNSA 1.0 and 2.0 use the same symmetric cryptography

- Grover's algorithm, discovered in 1996, provides an early example of a quantum speed-up with very broad applicability, giving "quadratic speed-up" to a many computing problems

- By 1999 there was a proof that a quantum computer can't solve that broad problem faster than Grover

- This simultaneously gives us:
  - The correct post-quantum key size for symmetric cryptography, like AES
  - Tells researchers the sorts of problems to use for the basis for post-quantum public key

Broad goals with CNSA 2.0 selections

SECURITY

Data must be secured for a long time horizon against a robust set of threats

SIMPLICITY

It must be as easy as possible for our users to comply with our requirements

VALIDATION

It should be simple for our users to validate that their systems comply with NSA guidance

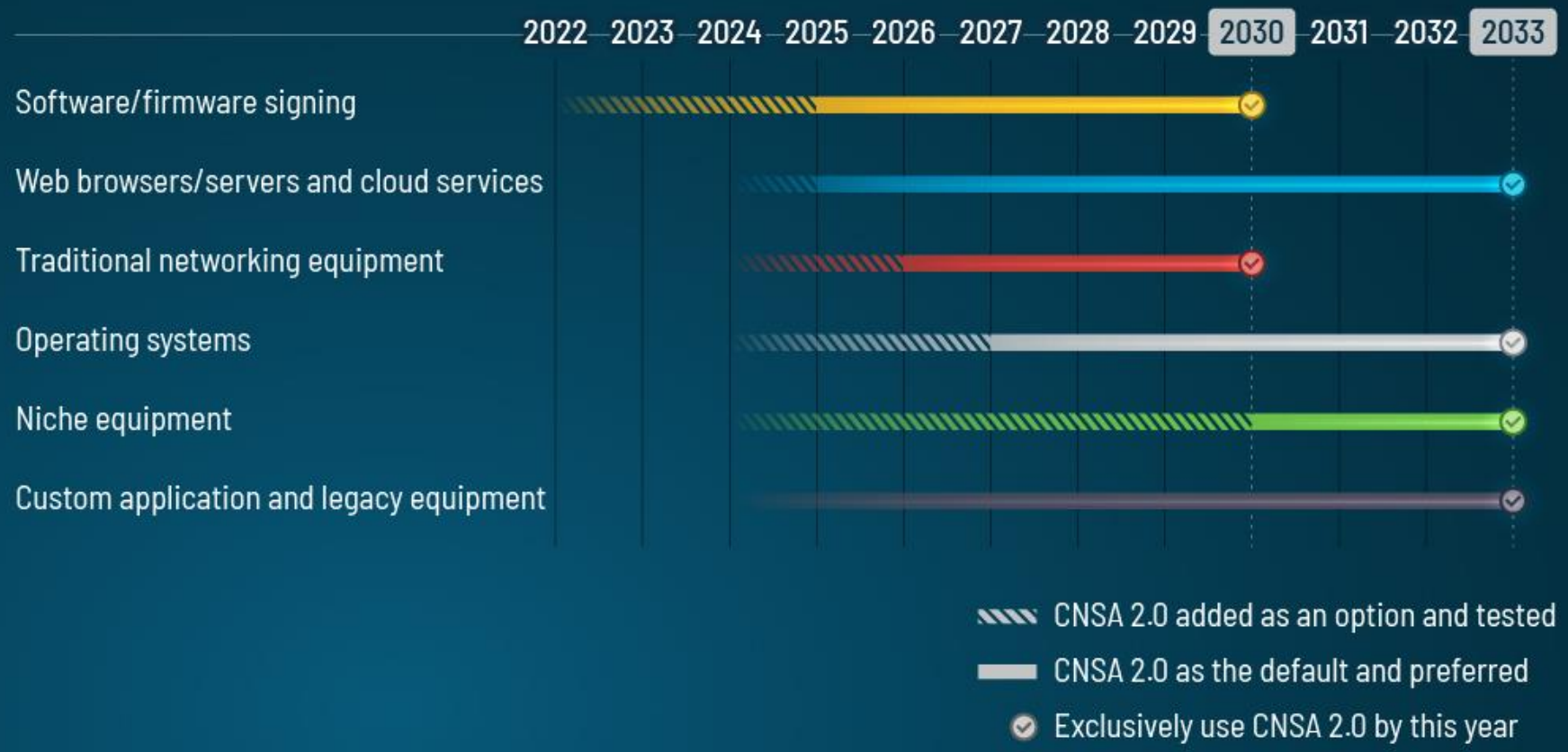
UNIVERSALITY

The requirements should cover the diverse set of use cases that make up the US National Security arena

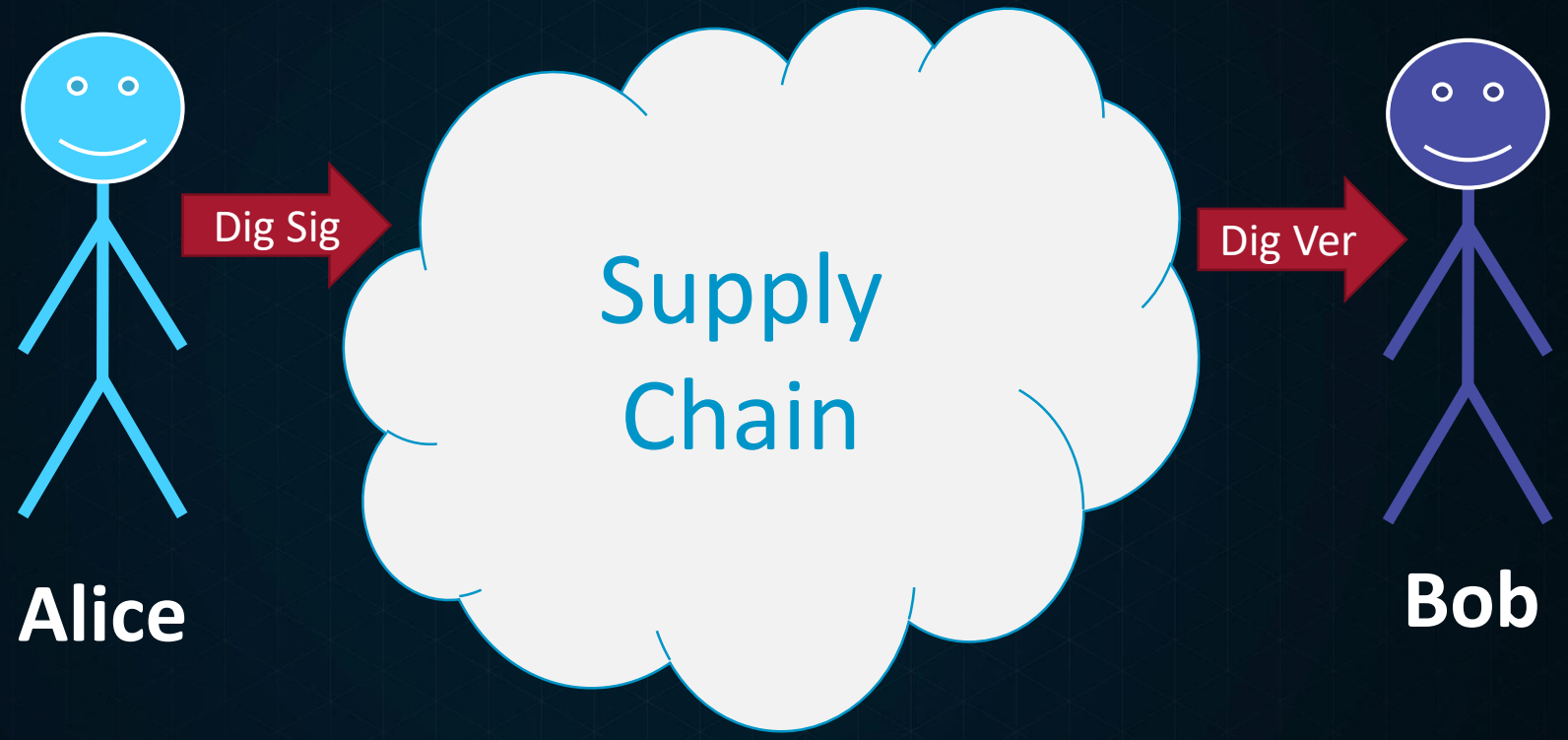
EASE OF ACQUISITION

It should not be difficult to comply while staying within normal acquisition processes

CNSA 2.0 Timeline



Cybersecurity ramifications of quantum computing



Without this verification, a cyber actor at any point in the supply chain process could substitute malicious code without detection.

Software and Firmware signing

Authentication of software and firmware is a critical part of the transition

- Hardware roots of trust must be secure for the life of the hardware, so they must transition sooner
  - For many systems this can easily mean a lead time of a decade
  - These systems, with very controlled upgrade paths are a great usecase for the hash-based signatures that NIST has already standardized: LMS and XMSS.
  - NSA expects to update Protection Profiles soon so our customers can purchase equipment signed with LMS/XMSS as long as the algorithm has been NIST CAVP certified.
- For software systems that expect to sign large volumes of code from many different sources, ML-DSA may be a better choice
  - These system, with their high degree of agility are precisely those that may be able to upgrade their root of trust faster
  - Standardized/Validated ML-DSA is not expected to be immediately available, and so this path should only be taken if a few-year delay will not impact transitioning previously deployed gear.

Quantum Resistant Cryptography, not Quantum Cryptography

- Quantum Resistant Cryptography is replacements for common public key functionality. Upgrades to hardware may be required due to larger bandwidth or processing, but there is a well-worn path for algorithmic upgrades.
  - Transition is similar to the SHA1 to SHA2 transition or DES to AES transition
- The field of quantum cryptography involves specialized hardware using the physics of quantum mechanics to protect the confidentiality of sensitive information. The most common example today uses quantum physics to distribute keys for use in a traditional symmetric algorithm, known as “quantum key distribution” or QKD.
  - Distinct from quantum computing, though both use quantum mechanics
  - QKD has been demonstrated for a long time
- QKD is not allowed on to protect National Security Systems after an analysis of practical security issues
  - QKD requires special purpose equipment
    - This equipment does not have any validation standards and relies on unique physical properties
  - No standards for interoperability
  - Very high cost/infrastructure
    - Either insider threat or limited use
  - Denial of Service issues are unavoidable

Questions?