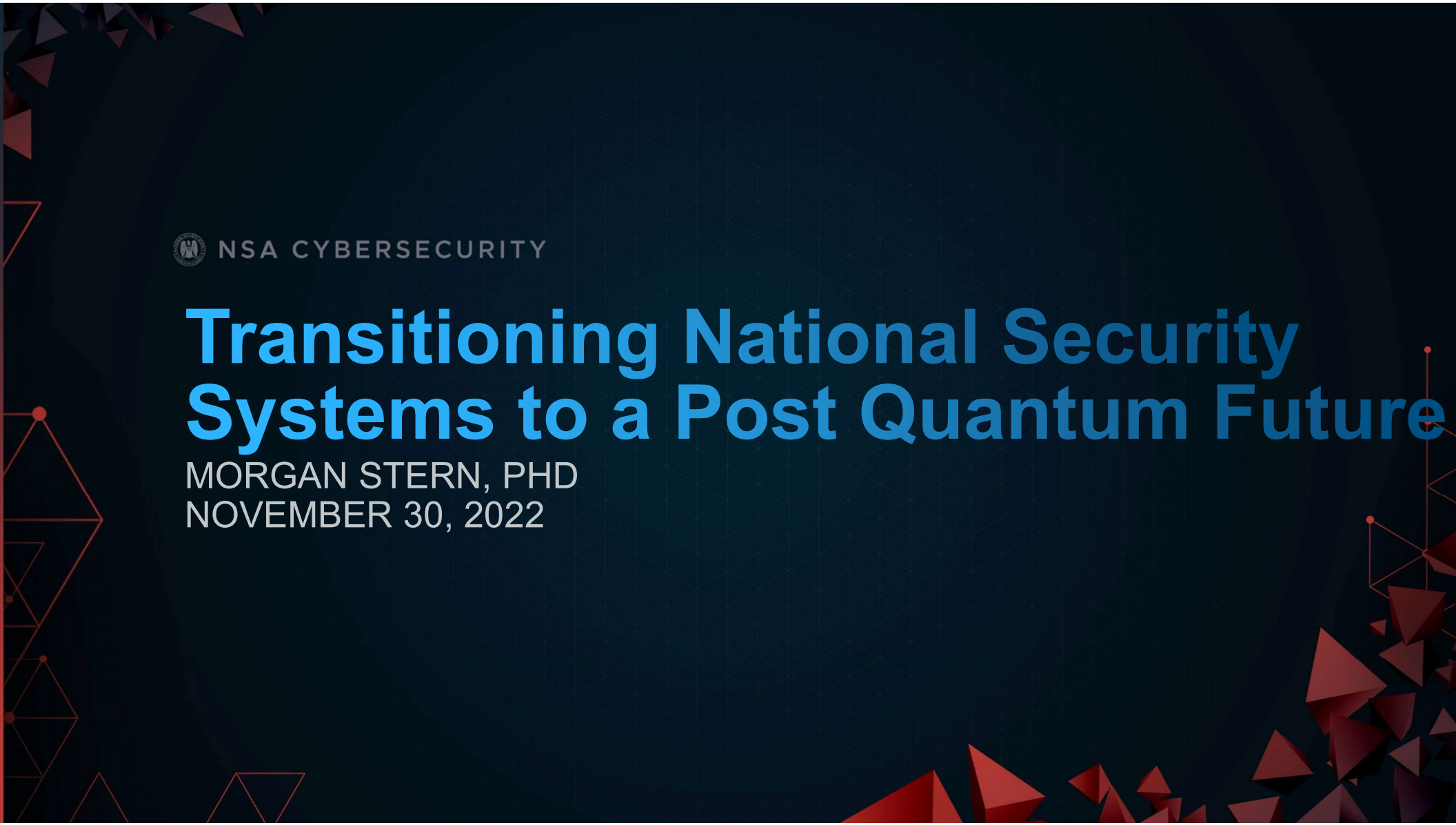

NSA CYBERSECURITY
Transitioning National Security Systems to a Post Quantum Future
MORGAN STERN, PHD
NOVEMBER 30, 2022

What is a National Security System?

The Director of NSA serves as the National Manager for US National Security Systems, giving NSA the authority to set requirements for cryptography across this area. This is a key part of NSA's Cybersecurity mission.

Most systems run by the Department of Defense or Intelligence Community fall under this "National Security System" classification.

- Department of Defense has well over a million employees who need secured communications with minimal downtime, with many deployed to locations across the world.
    - NIPRNet, which has been up since the original ARPANET
- Classified networks
- Industrial control systems owned by Department of Defense
- GPS
- Weapon systems

A little history

- 2001: CNSSP-11 lays out that commercial-off-the-shelf products intended to protect National Security Systems must be validated using the FIPS and NIAP processes
- 2005: Suite B announced, laying out the use of commercial standards for public key to be used to protect National Security Systems
- 2016: CNSSP-15 updated to address the quantum threat, and introducing CNSA 1.0
- May 2022: National Security Memo 10 signed making it an aim of US to be off quantum vulnerable crypt by 2035
  - Calls out to several cybersecurity agencies across the US Government to work in their area of responsibility to ensure a timely transition: NIST, CISA, OMB, ONCD, NSA
  - Calls out NSA to make standards for NSS and give a timeline for deprecation of quantum vulnerable systems
- September 2022: CNSA 2.0 released laying out how to achieve quantum resistance in NSS

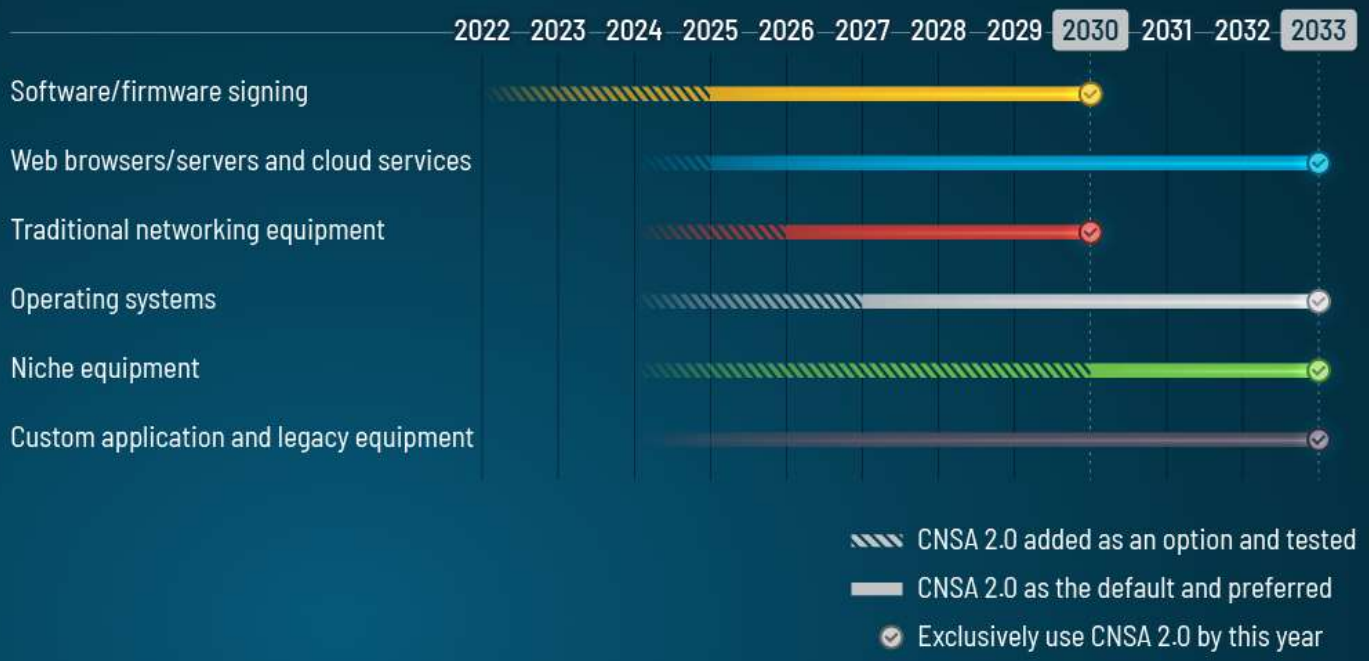
Commercial National Security Algorithm (CNSA) 2.0 Suite

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	Kyber (Level V)	TBD
Digital Signature	RSA-3096 or ECDSA P-384	Dilithium (Level V)	TBD
Software/Firmware Signature	RSA-3096 or ECDSA P-384	LMS or XMSS (LMS 256-192 recommended)	SP 800-208

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
- Ease of acquisition: It should not be difficult to comply while staying within normal acquisition processes
- Universality: The requirements should cover the diverse set of use cases that make up the US National Security arena

CNSA 2.0 Timeline



Example component of an NSS system: Common Access Cards

- Access to NIPR requires an active Common Access Card
  - Adheres to PIV standard, FIPS 201-3
- Adding quantum resistance
  - FIPS 201-3 must be updated to point to Dilithium and Kyber standards before any transition can occur
  - Smart card manufacturers will need to add the new Kyber/Dilithium functionality and get it FIPS validated
  - DoD PKI would need to stand up a root CA running Dilithium
  - Services would have to purchase a large number of physical smart cards
  - Services would need to verify all the platforms that rely on the cards can handle the new hardware
  - Users would physically receive new cards in person as their old ones expire
  - System is secured only when last quantum-vulnerable root CA expires

Decisions made now will dramatically impact how fast we can move over the next decade

- The diligence of the community in evaluating proposed post-quantum standards dictates how fast the standard will be able to be finalized
- The United States Government cannot start acquiring gear until independent testing labs can certify the standards, so standards written in an easier-to-certify fashion will speed government adoption
- Speed of integrating Kyber and Dilithium into existing higher-level standards impacts when the quantum threat is mitigated in practice
  - This requires prototyping, and that prototyping often does not require finalized standards

Speeding up adoption: Reuse development/validation work whenever possible

It's paramount to revalidate legacy systems before things are reused, but broadly:

- If a system can use a standardized algorithm, it is nearly always easier to do so
- If a system can reuse a FIPS validated module, that is nearly always cheaper and faster to deploy
- If a system has hardware acceleration for an algorithm, it is preferable to reuse that
- If a DRBG is being used somewhere within a standard, it is always simplest if it is a standardized one
    - If a standardized DRBG is going to call a primitive, it is always simplest if it is a standardized one

Speeding up adoption: Reuse infrastructure whenever possible

- We find users who often forget about interoperability until they need it
  - A reason to minimize the number of choices
- Funding cycles last years
  - Making two consecutive changes to a key agreement in one system can easily take several times as long as a single change
- Authentication often takes much longer to upgrade, so several algorithms will need to continue to be supported
  - Infrastructure is the last thing to upgrade away from legacy support
    - Interoperability with legacy devices breaks when infrastructure ends support
    - As end-devices upgrade away from legacy support, legacy gear becomes less and less interoperable
  - Customers still need SHA-2 for signing until RSA leaves interoperability

Example of Authentication Delays: SHA-1 versus SHA-2

- In 2005, Wang, et al. described a subexhaustive collision in SHA-1
  - SHA-2 had been standardized in 2001
- NIST formally deprecated SHA-1 in 2011
- NIST requested comments on removing SHA-1 from FIPS 180-4 in June 2022

Prototyping to buy down risk

- What products will these fit into
- Numerous further standards necessary for any commercial product
  - RFCs for CNSA-compliant TLS, IKE, SSH
- New capabilities should make sure there is a quantum resistant option
- Vendors need to start prototyping to understand potential issues

CNSA 2.0: Transitioning to a quantum-resistant future

- The quantum threat is real and we need to modernize ourselves to protect ourselves.
- We know from past experience that transitions take time, so we need to start planning now so we can start executing as soon as standards are completed.
- To be successful, we must collaborate across the entire ecosystem and each partner from industry, government, and academia will bring a unique perspective.
- Judicious choices today will lay the groundwork for a faster and smoother transition over the coming decade as standards are finalized.

Questions?