QR in NSS (Especially in CSfC)

(U) Bill Layton

Technical Director, Cryptographic Solutions

NSA's Role

From "General Commercial" to "Extra Special" NSA's responsibilities include

- Security of the Defense Industrial Base (guidance and services)
- Security of commercial security products used on National Security Systems (typically through NIAP)
- Solutions that protect classified information with commercial products (through the Commercial Solutions for Classified program, or CSfC)
- Government specified equipment for high assurance and/or military command and control functions (made with many commercial parts)

QR: How do we get there?

Mandate

Math Problem

- New Public Key
- Symmetric Options

Math Standards

Crypto Libraries

Standard Protocols

Proprietary and Niche Protocols

Module Validation

- FIPS
- NIAP
- CSfC

Configuration Guidance

Looking Deeper

Underlying Infrastructures

The Easy Ones in 2024

Mandate: NSM-8 and NSM-10, plus broad community agreement

Math Problem: Solved. New QR Cryptomathematics has been developed

Math Standards: Solved.

- NIST draft from 2023 becomes standard in 2024
- Symmetric Key is long established
  - Management is tricky and may need help to scale

Crypto Libraries: Broad incorporation underway already

Protocols in 2024

(D)TLS is ready but TLS 1.3 support will (probably) be required for QR

IPSec updates are finished, but the changes are more significant

WiFi will take longer, but it has limited quantum risk in the first place

Niche protocols (ssh, secure messaging apps, etc.) will be updated

- IETF pquip group covering the majority of standards
- Other protocols generally are updating smoothly

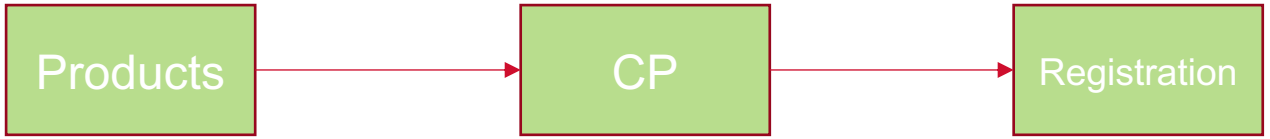
Many protocols rely on (D)TLS (e.g. MACsec) and need no extra work

Validation

Standing up validation takes time

For Products:

For CSfC Solutions



Today and Near Future Expectations

CSfC Symmetric Annex already exists

- Without improved key management standards scaling is hard
- Use based on risk and sensitivity

PP's update in synch with FIPS validation availability

CP's update with PP updates

Deployed solutions update with CP updates and regular renewal process

Start looking at the harder problems of more hidden cryptography

Looking Deeper/Underlying Infrastructures

Full QR will demand expansion of scope

O/S and driver patching

Software Product Patching

Firmware/Microcode update

Proprietary management protocols

Hardware root of trust (TPM)

Multi-factor authentication

- CAC/PIV/FIPS 201 updates will take time
- Large PKI updates will take longer
- PKI standards will take time in general, but CSfC PKI's might be faster

The Pain of Hardware

Chip development timelines are long

- CNSA rollout has already had to accommodate
  - ASIC's for embedded encryption
  - WiFi chipsets

Post-quantum algorithms may require some physical re-engineering

- Workspace on an IoT device/Smartcard may require expansion
- Low-powered comms may require adaptation

Vendor Encouragement

Expect CNSA 2.0 requirements to be in place quickly

- Mandates roll out once some products appear, so don't be late

Start looking through your systems for "hidden" cryptography

- Software/firmware updates
- Platform Integrity

Engage with the community

- NIST's NCCoE is a good place to start

(U) **Questions?**

nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources