QUANTUM COMPANIES — GUIDE

Post-quantum cryptography migration timeline

NIST FIPS 203/204/205 (ML-KEM, ML-DSA, SLH-DSA), NSA CNSA 2.0 and US OMB M-26-15 deadlines for federal and commercial migration.

Updated November 1, 2026

The US government has established mandatory timelines for migrating to post-quantum cryptography (PQC). Three NIST FIPS standards (August 2024), NSA CNSA 2.0 (advisory September 2022, FAQ updated December 2024) and OMB M-26-15 (June 2026) define the requirements and deadlines.

NIST FIPS standards (August 2024)

| Standard | Algorithm | Type | Primary use | Status | |---|---|---|---|---| | **FIPS 203** | ML-KEM (CRYSTALS-Kyber) | Key encapsulation mechanism (KEM) | Key establishment, TLS, VPN, SSH | **Final** — deploy now | | **FIPS 204** | ML-DSA (CRYSTALS-Dilithium) | Digital signature | Certificates, code signing, authentication | **Final** — deploy now | | **FIPS 205** | SLH-DSA (SPHINCS+) | Stateless hash-based signature | Firmware signing, long-term validity | **Final** — deploy now |

Source: NIST PQC Standards — fetched 2026-11-01.

Additional algorithms in standardization:

- **Falcon / FN-DSA** (digital signature) — selected for standardization, not yet a final FIPS.
- **HQC** (KEM) — selected for standardization, not yet a final FIPS.

NSA CNSA 2.0 requirements (advisory September 2022, FAQ V2.1 December 2024)

CNSA 2.0 (Commercial National Security Algorithm Suite 2.0) mandates PQC for National Security Systems (NSS). NSA requires the highest parameter sets at all classification levels.

| Function | Algorithm | Standard | Status for NSS | |---|---|---|---| | Key establishment | ML-KEM-1024 | FIPS 203 | Required | | Digital signatures | ML-DSA-87 | FIPS 204 | Required | | Software and firmware signing | LMS or XMSS (single-tree) | NIST SP 800-208 | Approved; support and prefer from 2025, exclusive use by 2030. ML-DSA-87 also approved once validated implementations exist | | Stateless hash-based signatures | SLH-DSA | FIPS 205 | **Not approved for NSS** under CNSA 2.0 |

Enforcement dates (CNSA 2.0 FAQ V2.1):

- **December 31, 2025**: no mandatory transition before this date. Systems validated under a NIAP or CSfC profile stay approved until their validation ends.
- **January 1, 2027**: procurement gate. All new NSS acquisitions must support CNSA 2.0 unless

an exception applies.

- **December 31, 2030**: equipment and services that cannot support CNSA 2.0 must be phased out.
- **December 31, 2031**: CNSA 2.0 mandatory across all NSS unless explicitly exempted.

Category dates (original advisory): software and firmware signing: support and prefer by 2025, exclusively use by 2030. Web browsers, servers and cloud services: 2025 / 2033. Traditional networking equipment: 2026 / 2030. Operating systems: 2027 / 2033. Niche equipment: 2030 / 2033. Custom applications and legacy equipment: update or replace by 2033.

Source: NSA CNSA 2.0 FAQ — fetched 2026-11-01; NIST IR 8547 — fetched 2026-11-01.

US OMB M-26-15 (June 24, 2026)

OMB Memorandum M-26-15 "Execution of the Migration to Post-Quantum Cryptography" implements the June 22, 2026 executive order and directs federal civilian agencies. It does not apply to National Security Systems; those follow the CNSA 2.0 track.

| Requirement | Deadline | |---|---| | Submit a PQC Migration Plan to OMB and ONCD | **120 days** — by October 22, 2026 | | Mitigate as much quantum risk as feasible in agency systems | **December 31, 2030** | | Multiyear migration, five phases | **2026–2035** |

The initial plan must cover the first three migration phases and a TLSv1.3 testing and deployment timeline. It must include risk-based prioritization, phased timelines, an automated cryptographic inventory, a crypto-agility architecture, third-party and cloud coordination, funding estimates and named governance roles.

The related executive order (EO 14412) requires federal high-value assets and high-impact systems to migrate by 2030 for key establishment and by 2031 for digital signatures. The earlier OMB M-23-02 (November 2022) started agency planning and inventory; M-26-15 sets execution deadlines.

Source: OMB M-26-15 — fetched 2026-11-01; NIST report on IR 8547 — fetched 2026-11-01.

Migration phases (OMB M-26-15)

| Phase | Timeline | Actions | |---|---|---| | **1 — Strategy, planning and discovery** | 2026–2027 | Cryptographic inventory (including HVAs and high-impact systems), risk assessment, governance, further migration plans | | **2 — Pilots and early migration** | 2027–2028 | Pilots and early migration of prioritized systems; refine the plan | | **3 — Prioritized migration** | 2028–2030 | Migrate key establishment for HVAs, high-impact and highly-sensitive systems to PQC | | **4 — Signature migration** | 2031 | Migrate digital signatures for the same prioritized systems to PQC | | **5 — Full migration** | 2035 | Complete the migration of remaining systems |

NIST IR 8547 (final, October 2026) sets the standards timeline: NIST deprecates quantum-vulnerable public-key cryptography after 2030 and disallows it under NIST standards and guidelines after 2035. Separately, Executive Order 14306 requires agencies to support TLS 1.3 or a successor version as soon as practicable and no later than January 2, 2030.

Compliance checklist for buyers

- [ ] Ask vendors for FIPS 203/204/205 validation certificates (CMVP)

- [ ] Confirm TLS 1.3 hybrid key exchange (X25519+ML-KEM, etc.) support
- [ ] Verify X.509 certificate support for ML-DSA and SLH-DSA
- [ ] Require crypto-agility: ability to swap algorithms without firmware replacement
- [ ] Check CNSA 2.0 compliance if selling to US government / NSS
- [ ] Plan for stateful hash-based signature (LMS/XMSS) key management where required
- [ ] Budget for HSM/firmware updates and certificate re-issuance

Sources

- NIST FIPS 203 (ML-KEM) — fetched 2026-11-01.
- NIST FIPS 204 (ML-DSA) — fetched 2026-11-01.
- NIST FIPS 205 (SLH-DSA) — fetched 2026-11-01.
- NSA CNSA 2.0 FAQ — fetched 2026-11-01.
- NIST IR 8547: Transition to PQC Standards — fetched 2026-11-01.
- OMB M-26-15 — fetched 2026-11-01.
- NCCoE Migration to PQC project — fetched 2026-11-01.

For planning only — not legal or compliance advice. Confirm your obligations with counsel and the cited authorities.

Frequently asked questions

When must federal agencies migrate?

OMB M-26-15 (June 24, 2026) requires each federal civilian agency to submit a PQC Migration Plan to OMB and ONCD within 120 days (by October 22, 2026) and to mitigate as much quantum risk as feasible by December 31, 2030. National Security Systems follow NSA CNSA 2.0 instead.

What algorithms are approved for CNSA 2.0?

NSA CNSA 2.0 (FAQ V2.1, December 2024) requires ML-KEM-1024 (FIPS 203) for key establishment and ML-DSA-87 (FIPS 204) for digital signatures in National Security Systems, with LMS or XMSS (single-tree, NIST SP 800-208) for software and firmware signing. SLH-DSA (FIPS 205) is a NIST standard but is not approved for NSS under CNSA 2.0.

Do commercial vendors need to comply?

Commercial vendors selling to US federal agencies must comply with CNSA 2.0 for classified/national security systems. NIST standards (FIPS 203/204/205) are mandatory for federal agencies and recommended for critical infrastructure. Many industries (finance, healthcare) are adopting voluntarily.

What about Falcon and HQC?

Falcon (digital signature) and HQC (KEM) were selected for ongoing standardization (Round 4). They are not yet FIPS-standardized. Do not deploy in production until final FIPS publications.