MOBILALLY WHITE PAPER SERIES · No. 1

# The 2030 Deadline Is Coming for Legacy Infrastructure

*Post-quantum mandates are now law, policy, and procurement reality. The hardest part of the migration is not the algorithms — it is the installed base.*

## The deadline wave

In a five-week window in mid-2026, the United States government converted post-quantum cryptography from a research roadmap into an enforceable schedule. A June 22 Executive Order directs high-value federal systems to complete the transition to post-quantum cryptography by **December 31, 2030** — pulled forward from a prior planning horizon near 2035. The following day, the Department of War published its Post-Quantum Cryptography Strategy: every system supports PQC or begins phase-out by the end of 2030, and every system runs it by the end of **2031**. The strategy names *cryptographic agility* — the ability to change cryptographic algorithms after deployment — as a strategic goal, and commits the Department to rapid vetting of commercial solutions.

The regulatory machinery beneath those dates was already moving. NIST finalized its first PQC standards in 2024 and has published formal guidance on achieving cryptographic agility. In September 2026, the national validation program moves every remaining FIPS 140-2 certificate to historical status — a forcing function that touches every legacy cryptographic module in federal service. For the automotive and industrial world, UNECE R155/R156 and ISO/SAE 21434 already make provable cyber and update management a condition of market access in Europe.

## Why the urgency is real today: harvest now, decrypt later

The threat model that drives these deadlines does not wait for a quantum computer to exist. Adversaries intercept and store encrypted traffic today, knowing that data with a long shelf life — health records, financial archives, intellectual property, government communications, infrastructure telemetry — will still be sensitive when a cryptographically relevant quantum computer arrives. Every day of delay adds to the archive an adversary will eventually open. The migration deadline is 2030; the exposure began years ago.

The timeline itself keeps compressing. Published research in 2025 and 2026 reduced the estimated quantum resources required to break RSA-2048 and 256-bit elliptic-curve cryptography by roughly twenty-fold each — improvements achieved on paper, through better algorithms, independent of any progress in quantum hardware. Standards officials have said publicly that these results should accelerate, not merely confirm, migration plans.

## The hard part is the installed base

For a cloud service, PQC migration is a software update. For the systems that run the physical world, it is not. Four properties make legacy and edge infrastructure the hardest mile of this transition:

- **Lifecycles measured in decades.** Vehicles, industrial controllers, medical devices, utility equipment, and defense platforms serve 10–25 years. Hardware fielded this year will still be in service on the far

side of every deadline above — and on the far side of standards that do not exist yet.

• **Fixed-function cryptography.** Much of the installed base anchors its security in silicon that cannot change algorithms after manufacture. When the mandated algorithm changes, the options are replacement or non-compliance.

• **Recertification cost.** Regulated systems — aviation, automotive, medical, defense — cannot simply patch cryptography; changes ripple into type approval, safety cases, and accreditation. The U.S. Air Force has stated on the record its strong interest in mechanisms that protect difficult-to-modify legacy systems *without requiring complete recertification*.

• **Divergent requirements.** Germany's BSI mandates hybrid classical-plus-PQC constructions; U.S. national security guidance moves to standalone PQC; in July 2026, ISO standardized a code-based algorithm that NIST had passed over. A device fielded into multiple jurisdictions must satisfy futures that already disagree with each other.

Together these produce the trap the industry is only now naming: systems become *cryptographically fixed at exactly the moment cryptography must become fluid*. Even the world's most widely deployed root of trust — PC Secure Boot — is publicly struggling through a routine certificate rollover on older machines in 2026. That is a classical transition, on the best-supported platform on earth. The post-quantum transition, on constrained embedded fleets, will be strictly harder wherever the root cannot be updated.

***"Cryptographic agility is no longer a preference. For any system that will still be in service in 2030, it is the compliance strategy."***

## What operators should do now

• **Inventory cryptography as an asset class.** Federal agencies are already required to; every infrastructure operator should. You cannot migrate what you have not mapped — algorithms, key stores, certificate chains, and the hardware each depends on.

• **Triage by data lifetime, not system age.** The first systems to migrate are those protecting data that must remain confidential past 2030 — regardless of how new the system is.

• **Make agility a procurement requirement.** Ask every vendor the same question: *when the algorithm changes after deployment, what changes — a configuration, or the hardware?* Contracts signed in 2026 will govern equipment still fielded in 2040.

• **Demand hardware-anchored agility, not software-only agility.** Software layers can swap algorithms, but keys generated and held in accessible memory trade the quantum threat for the physical-access threat. The durable posture pairs updatable cryptography with a hardware boundary for entropy and key custody.

## About MobilALLY

MobilALLY LLC is a service-disabled veteran-owned small business building hardware-rooted, post-quantum cryptographic modules for edge, mobility, and defense platforms — engineered on the principle that the hardware root of trust itself must be agile: field-updatable cryptography anchored by hardware entropy and isolated key custody, so that long-lived systems can meet the deadlines above without redesign. Learn more at www.mobilally.io.

## Sources

Executive Order, “Securing the Nation Against Advanced Cryptographic Attacks,” June 22, 2026 (whitehouse.gov).

Department of War, Post-Quantum Cryptography Strategy, June 23, 2026 (dowcio.war.gov); coverage: DefenseScoop, June 25, 2026.

NIST CSWP 39, Considerations for Achieving Cryptographic Agility, December 2025; NIST FIPS 203/204/205 (2024).

CMVP transition of FIPS 140-2 certificates to historical status, effective September 21, 2026.

DoW SBIR 2026 BAA, Topic DAF26BZ03-NV017 (QSPARX), published Topic Q&A;, June 2026.

IEEE Spectrum, “Independent Labs Crack Google’s Secret Cryptography Work,” July 7, 2026.

ISO/IEC 18033-2 amendment incorporating Classic McEliece, July 2026; coverage: The Quantum Insider, July 15, 2026.

Elektor, “Automotive crypto-agility for ECUs” (IAV GmbH), July 20, 2026.

EE Times, “Post-Quantum Cryptography Incorporated into SoCs via eFPGA,” July 20, 2026.