Digi International – Preliminary Position on Post-Quantum Cryptography (PQC)

Public-Facing Statement | Version: 1.1 | Date: January 2026

Executive Summary

Quantum computing may, in the future, affect certain widely used public-key cryptographic algorithms. Digi International is monitoring the evolving standards landscape and preparing for a transition through crypto-agility, robust implementation practices, and lifecycle support for devices and services.[1]

Because post-quantum standards and ecosystem interoperability continue to mature, Digi International's approach is risk-based and phased. We will align our adoption plans with broadly accepted standards and customer requirements, especially for long-lived IoT deployments and regulated environments.[1]

Regulatory- and Standards-Aware Approach (Public Summary)

- Standards alignment: We track guidance and standards from recognized bodies (including NIST) and plan to incorporate standardized, interoperable approaches as appropriate.[1]
- U.S. Government readiness: For customers that require government-aligned cryptography profiles, we monitor relevant U.S. Government guidance (including NSA CNSA Suite 2.0) to support long-term transition planning.[2]
- EU cybersecurity expectations: We recognize that EU frameworks emphasize risk management, secure development, vulnerability handling, and the appropriate use of cryptography and encryption. Digi International's product security program is designed to support these expectations across the product lifecycle.[3][4]

Our Current PQC Position

1) Crypto-agility first

Digi International prioritizes crypto-agile designs and upgrade paths so cryptographic algorithms and parameters can be updated as standards mature and interoperability improves.[1]

2) Phased, use-case-driven adoption

When customer needs and threat models warrant (for example, long-lived confidentiality requirements), we will evaluate phased approaches, including transition strategies that maintain compatibility with existing systems while enabling post-quantum readiness.[1]

3) Implementation security and lifecycle support

Digi International emphasizes secure implementation and lifecycle practices—secure boot and firmware authenticity controls, secure key management, and timely vulnerability handling and updates—because these are essential to real-world resilience for embedded and IoT systems.[4][5]

What This Means for Customers and Partners

- No immediate customer action is required solely due to PQC. We continue to support current, standards-based cryptographic protections while tracking PQC standardization and adoption guidance.[1]
- For regulated or long-lifecycle deployments, we support risk-based planning and will communicate relevant roadmap updates through product documentation and the Digi Security Center.[5]

Important Notice (Safe Harbor)

Post-quantum cryptography standards, implementations, and recommended practices are evolving. This public statement reflects Digi International's current view as of the date above and is provided for informational purposes only. It does not constitute a commitment to specific cryptographic algorithms, certifications, or timelines. Adoption decisions will remain standards-aligned and use-case driven.

References

[1] NIST CSRC, "Post-Quantum Cryptography" (includes FIPS 203 ML-KEM, FIPS 204 ML-DSA, FIPS 205 SLH-DSA). https://csrc.nist.gov/projects/post-quantum-cryptography

[2] U.S. National Security Agency, "Commercial National Security Algorithm Suite 2.0" (CNSA 2.0) cybersecurity advisory. https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

[3] NIS2 Directive (Article 21) – cybersecurity risk-management measures including cryptography/encryption policies. https://www.nis2-info.eu/article-21-cybersecurity-risk-management-measures/

[4] EU Cyber Resilience Act – summary briefing referencing Regulation (EU) 2024/2847 and lifecycle security obligations. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI%282022%2973 9259_EN.pdf

[5] Digi International Security Center (security advisories) and Support Policy (firmware maintenance / patching posture). https://www.digi.com/resources/security ; https://www.digi.com/support/support-policy