Cybersecurity Coalition

29 September 2025

VIA ELECTRONIC SUBMISSION

Re: Survey - EU Roadmap on Post-Quantum Cryptography

The Cybersecurity Coalition ("the Coalition") submits the following comments in response to the European Union Network and Information Systems (NIS) Cooperation Group's *Survey on the EU Roadmap on Post-Quantum Cryptography* ("the Roadmap").

The Coalition is composed of leading companies with a specialty in cybersecurity products and services, dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management.

The Coalition included "proactively manag[ing] the transition to post-quantum cryptography" as one of the 12 policy recommendations in its 2024-2029 EU Cyber Policy Roadmap. Accordingly, we are delighted to see the European Union (EU) take proactive steps to ensure that government institutions, Member States, critical infrastructure, and other organizations are ready for the transition to post-quantum cryptography (PQC). We offer the following comments and recommendations in support of these efforts.

What are the most useful parts of the roadmap?

The Coalition applauds the NIS Cooperation Group's development of the Roadmap as a means to synchronise the EU's transition to PQC. Specifically, the Coalition appreciates the focus on "public and administration entities and other critical infrastructures … in the scope of the NIS2 Directive," highlighted in Section 3.1. This scoping will facilitate a streamlined implementation process that complements rather than conflicts with existing EU directives and regulations. For example, national governments will be able use existing contacts built during their NIS 2 implementation campaigns and avoid the need to devise new strategies for outreach. Moreover, by helping to align the national policies and timelines of all 27 Member States, the Roadmap will avoid the creation of duplicative – or worse conflicting – requirements. This will also simplify the process for industry, reduce the likelihood of delays, and accelerate implementation in those Member States with fewer resources to commit to the transition.

The Coalition also strongly supports the NIS Cooperation Group's efforts to align the Roadmap with non-EU jurisdictions. Specifically, we appreciate the Roadmap's compatibility with the United Kingdom National Cyber Security Centre's (NCSC) *Timelines for migration to post-quantum cryptography* and the United States' *National Security Memorandum on*

Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10), each of which target 2035 for complete migration of all systems, services and products under their respective jurisdictions. This alignment with non-EU jurisdictions is essential given the global nature of the cybersecurity threat posed by cryptographically-relevant quantum computers (CRQCs). A consistent global implementation prevents fragmentation of standards and inconsistent security postures, which could otherwise create weak points between different jurisdictions, sectors and organisations. Moreover, it enables multinational companies operating between jurisdictions to apply a coherent policy across all their assets. This coherence makes quantum safe systems easier to maintain, which itself is advantageous for security. It is also more cost effective, enabling finite cybersecurity budgets to be reinvested into other pressing priorities, such as implementing requirements under EU legislation like the NIS 2 Directive and the Cyber Resilience Act (CRA). Finally, harmonised international approaches align with the European Commission's broader political priorities on simplification and regulatory coherence under the current mandate.

What areas of the roadmap need improvement or clarification? Please explain your answer

In its advocacy, the Coalition reaffirms the notion that the digital environment is inherently borderless with internet traffic routinely flowing between different jurisdictions. As such, we believe it is essential that the algorithms that protect this traffic are harmonised wherever possible. Requiring encryption to be altered as data crosses borders to comply with differing but similar standards would not only introduce latency and complexity in implementation, but could also increase security vulnerabilities. Therefore, the EU must allow for flexibility in choice of internationally-standardised quantum-safe algorithms to ensure data can continue to flow without technical interruption.

In the current draft, the Roadmap says "at this point, this document does not contain detailed technical recommendations." The Coalition strongly urges the NIS Cooperation Group to maintain this flexibility, especially given the possibility that some PQC algorithms may have undiscovered vulnerabilities that become apparent after deployment. For example, two algorithms submitted to the United States' National Institute of Standards and Technology (NIST) for standardisation – Supersingular Isogeny Key Encapsulation (SIKE) and Rainbow – have already been broken. Therefore, to mitigate risk, the NIS Cooperation Group should accept a range of standardised, internationally-recognised options of PQC algorithms in later versions and additional parts of the Coordinated Implementation Roadmap envisioned in Section 3.1. These should align with the recommendations of global partners and allies and should not be unique to the EU.

The Coalition also recommends that the NIS Cooperation Group clarify its language around hybrid algorithms, noting use cases for which such algorithms may not be optimal. Whereas the Roadmap recommends the use of standardised hybrid solutions "whenever feasible and suitable," the United Kingdom's NCSC is more cautious in approach. In its August 2024 paper entitled "*Next steps in preparing for post-quantum cryptography*," NCSC argues that hybrid algorithms are "more complex to implement and maintain" and are less computationally efficient as compared to single algorithms. While NCSC acknowledges that hybrid

algorithms are useful in cases where there are concerns around "interoperability, implementation security, or constraints imposed by a protocol or system," their drawbacks mean that they should only be "used as an interim measure … within a flexible framework that enables a straightforward migration to PQC-only in the future." This view is reinforced by the United States National Security Agency's (NSA) December 2024 guidance entitled "*The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ*." Given the diverging approaches of EU partners, the Coalition urges the NIS Cooperation Group to adopt language that is more compatible with these jurisdictions in order to facilitate harmonisation. Moving forward, the Coalition also cautions against requiring the use of hybrid algorithms, which could affect interoperability.

Finally, the Coalition recommends that the NIS Cooperation Group reconsider its recommendation that the "PQC transition for high-risk use cases has been completed" by 31 December 2030. While a phased implementation approach with staged targets for low-, medium- and high-risk use cases is prudent in theory, it would be difficult in practice for the Union given that each Member State and/or critical infrastructure entity is ultimately responsible for its own implementation. A key issue here is the classification of particular use cases' risk levels. Although the Roadmap advises that organisations use *The PQC Migration Handbook* – jointly developed by the The Netherlands Organisation for Applied Scientific Research (TNO), the Dutch General Intelligence and Security Service's (AIVD) and the Centrum Wiskunde & Informatica (CWI) – to perform quantum risks analyses, it is likely that several Member States will recommend other alternative frameworks. Therefore, a use case defined as medium risk by one Member State framework – and thus subjected to the 2035 transition deadline – could be defined as high risk in another – and subjected to the 2030 transition deadline. In this case, multinational organisations would need to meet the highest common denominator. If even one Member State decides a particular use case is high risk, it will need to transition that system by 2030. Moreover, given how most multinational companies are structured, they would likely need to transition that use case across all their digital infrastructure for the Union. This could mean an unnecessarily expeditious transition for certain systems.

This problem is further exacerbated by the fact that national guidance on the PQC transition does not yet exist in many Member States and likely will not for several years. This means that some countries may classify use cases as high risk only a few years before the 2030 deadline. To address these challenges, the Coalition recommends that the NIS Cooperation Group adopt a unified transition objective of 2035 for all low-, medium-, and high-risk use cases. If the Group wishes to continue encouraging earlier action for high-risk use cases, it could follow the example of the UK NCSC, which encourages owners of large organizations and operators of critical national infrastructure systems to "carry out [their] early, highest-priority PQC migration activities" by 2031 without imposing a strict deadline. This approach would also align well with the other targets outlined in the Roadmap's *Next Steps*, which the Coalition fully supports.