ACM Europe Technology Policy Committee's response to a consultation on the recently adopted (20 January 2026) EC proposal for a Directive (aka Cybersecurity Act 2)

May 2026

Dr. Luigi Di Biasi, Dr. Achim Brucker, and Dr. Chris Hankin.

The Association for Computing Machinery (ACM) is the world's longest-established professional society of individuals involved in all aspects of Computing. It annually bestows the ACM A.M. Turing Award, often popularly referred to as the "Nobel Prize of Computing." ACM's Europe Technology Policy Committee ("Europe TPC") is charged with, and committed to, providing policymakers and the general public with sound technical information to support sound public policymaking. Europe TPC has previously responded to European Union stakeholder consultations in the context of the AI Act[1], the Data Act[2], the Digital Services Act[3][4], the Digital Citizen Principles[5], and the Cyber Resilience Act[6], amongst others[7]. ACM and Europe TPC are non-profit, non-political, and non-lobbying organisations.

Europe TPC supports amending Directive (EU) 2022/2555, given the pace of change in the cybersecurity threat landscape and major developments since 2022 that have enabled more advanced threats and expanded the potential attack surface. We welcome the inclusion of Digital Identity, Business Wallets, and submarine data transmission infrastructure in the proposed amendment. We also support the requirement that EU Member States include migration to post-quantum, or quantum-safe, cryptography in their national cybersecurity strategies.

Given the rapid rise in incidents of ransomware attacks over the last few years, efforts to harmonise and improve the collection of data related to these attacks are welcome.

Europe TPC welcomes the Commission's intention to develop guidelines to facilitate harmonisation and reduce unnecessary duplication in information requested from suppliers. We would also like to see the European cybersecurity certification scheme

[1] https://www.acm.org/binaries/content/assets/public-policy/europe-tpc-comments-ai-consultation.pdf
[2] https://www.acm.org/binaries/content/assets/public-policy/acm-eur-tpc-data-act-comments-13may22a.pdf
[3] https://www.acm.org/binaries/content/assets/public-policy/europetpc-digital-services-act-comments.pdf
[4] https://www.acm.org/binaries/content/assets/public-policy/acm-europe-tpc-dsa-comments.pdf
[5] https://www.acm.org/binaries/content/assets/public-policy/europetpc-comments-digital-principles.. Wepdf
[6] https://www.acm.org/binaries/content/assets/public-policy/acm-europe-tpc-cyber-reslience-comments-pdf
[7] https://www.acm.org/public-policy/public-policy-statements

include an appropriate certification scheme for companies in the supply chain, which might obviate the need for such questionnaires.

Whilst generally welcoming the proposed amendment to Directive (EU) 2022/2555, we have the following detailed comments:

1. **Amendment (1, Article 2, paragraph 2, point iii)**

   Removing micro and small-sized DNS service providers from the scope may reduce administrative burden, but it also creates a material resilience gap in an infrastructure layer that is inherently cross-cutting and frequently targeted. DNS service providers *(regardless of company size)* remain a critical part of the Internet (and of Autonomous Systems and so forth), and most of the currently deployed critical infrastructure (including billions of Internet of Things (IoT) and Operational Technology (OT) devices) rely on DNS for their configurations and operation. Compromise of authoritative DNS management, resolver infrastructure, or administrative interfaces can enable domain hijacking, traffic interception, malware distribution, or broad service disruption. Even if each small DNS service provider is individually "non-systemic," *the aggregated risk is not.* There is also the issue of no-longer-used domains potentially being transferred from large to small-sized DNS service providers.

   The proposal also appears to reduce direct supervisory coverage *without clearly articulating an alternative* mechanism to ensure a baseline of security for out-of-scope DNS providers. Also, relying primarily on supply-chain pressure from in-scope entities is unlikely to be a stable substitute. Despite the fact that the objective is to "reduce bureaucracy", this choice can lead to fragmented and inconsistent contractual demands (multiple questionnaires and bespoke audits) that instead *may increase costs for small providers* without guaranteeing the adoption of effective controls.

   A more coherent approach would preserve proportionality while avoiding a *"security vacuum"* by introducing a light, risk-based baseline for DNS providers outside the full NIS2 regime, combined with clear escalation criteria. Such criteria could be based on objective technical and operational factors, *for example, the scale of DNS zones managed*, the number of customers served, the presence of essential/important entities among customers, or the provider's role as a managed authoritative DNS operator.

2. **Amendment (2, Article 3, paragraph 1, point i)**

   Removing the wording “as well as DNS service provider” risks creating a regulatory and supervisory gap for a cross-cutting service layer that remains relevant for overall resilience. If this deletion is maintained, we would suggest clarifying which alternative mechanism will ensure a minimum baseline of cybersecurity for DNS providers that may fall outside the amended scope, in order to avoid a security vacuum and inconsistent downstream requirements driven only by contractual pressure.

3. **Amendment (2, Article 3, paragraph 4)**

   The mechanism still appears to lack a clear deadline for entities to submit the required information once they fall within scope. In addition, it may be useful to clarify that the information provided should be accurate and complete at the time of submission, to support reliable coordination across EU Member States and to minimise inconsistencies in the resulting registers.

4. **Other points (including the Explanatory Memorandum)**
   a. In the proposal, some key terms appear overly broad and could benefit from clearer anchoring to objective criteria. In particular, expressions such as sensitive information and data and Union critical infrastructure would be more actionable if aligned with existing EU definitions and, where needed, ***complemented by measurable threshold***s or references to established classifications, so that implementation is consistent across Member States.
   b. Where the text refers to an appropriate level of security, **it would be helpful to clarify what this means in practice**, for example, by indicating minimum baseline controls, assurance levels, or references to recognised standards and profiles. There is a risk of divergent interpretations and uneven security outcomes.
   c. On the post-quantum transition, the proposal would be strengthened by requesting that EU Member States define a concrete migration roadmap with indicative milestones and prioritisation criteria, given the long lead times for the cryptographic transition and the cross-border nature of digital identity ecosystems. For example, the German BSI sets 2031 as a deadline: "The sole use of classic key agreement mechanisms is only recommended until the end of 2031 (see

https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html, Section 2.1)" - compliance with these recommendations is required in a number of areas (not only in Germany).

d. If the objective is to reduce fragmentation and improve coordination, we would also encourage a more explicit commitment to standardised, interoperable information structures and a common repository or reference mechanism that prevents repeated ad hoc requests and supports timely aggregation and analysis at the Union level.
e. Also, whilst the focus on ransomware reporting is understandable, it may be useful to ensure that incident reporting and situational awareness mechanisms remain threat-agnostic and equally capable of capturing other high-impact scenarios, such as supply-chain compromise, identity takeover, or attacks affecting OT and critical services, to avoid blind spots in Union-wide risk assessment.
f. Finally, the 1 MW threshold for electricity producers may miss relevant risk cases. It is unclear what the rationale for this particular threshold is. We would encourage the Commission to consider additional objective criteria beyond nameplate capacity, for example: whether the installation is remotely operated, whether it is part of an aggregation scheme, whether it provides grid-support services, whether it is integrated with OT/SCADA systems, or whether many similar units are managed through the same platform or supplier. These factors can materially increase exposure and potential cascading effects even when each individual generator operates below 1 MW.