COMMENTS OF THE ACM EUROPE TECHNOLOGY POLICY COMMITTEE ON A EUROPEAN COMMISSION PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON HORIZONTAL CYBERSECURITY REQUIREMENTS FOR PRODUCTS WITH DIGITAL ELEMENTS[1]

The Association for Computing Machinery (ACM) is the world's largest and 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 objective technical information to policy makers and the general public in the service of sound public policymaking. ACM and Europe TPC are non-profit, non-political, and non-lobbying organizations. Europe TPC is pleased to submit the following comments in response to the European Commission proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act).[2]

Europe TPC supports the need for action at the EU level to increase the level of trust among users of products with digital elements as well as the attractiveness of products with digital elements whose intended or reasonably foreseeable uses include a direct or indirect logical or physical data connection to a device or network. We generally concur that horizontal legislation delineating cybersecurity requirements for such products is the correct approach towards achieving these twin goals. Europe TPC also wishes, however, to make the following specific recommendations for changes to the proposed Cyber Resilience Act (and associated documentation):

Recital 10

We are concerned that the exclusion of certain types of open-source software (OSS) from the Cyber Resilience Act may have unintended consequences, for instance by potentially encouraging some vendors to rely more heavily on OSS components to circumvent its requirements. We thus urge the Commission to expand the proposed Regulation's scope to, for example, encompass commercial software that relies on open-source software development kits or application programming interfaces that might be adversely affected by vulnerabilities in the underlying open-source SDK or API. This concern is not theoretical, as illustrated by the Log4J and SolarWinds examples.

---

[1] Europe TPC's Chair, Chris Hankin of Imperial College London, was the principal author of these comments. Also contributing were Europe TPC member Andrew McGettrick, and ACM members Advait Deshpande and Ricardo Ferreira.

[2] COM(2022) 454 final 2022/0272 (COD) Brussels, 15.9.2022

ACM Technology Policy Office
1701 Pennsylvania Ave NW, Suite 200
Washington, DC 20006

+1 202.580.6555
acmpo@acm.org
www.acm.org/public-policy

Recital 67
ACM Europe TPC welcomes the proposed use of bilateral Mutual Recognition Agreements for conformity assessment and the marking of regulated products as a mechanism to strengthen cyber resilience globally.

Article 6
Whilst Europe TPC acknowledges the need to identify critical products with digital elements, we note that the rationale for the Class I/II lists as set out in the Annex III is not clear. With the increasing rate of digitalisation, it is likely that these lists will change more rapidly than the proposed review process can accommodate. Thus, it may be preferable to use a higher level of abstraction in the categorisation. For example, in the "IACS category," systems are classified based upon whether they do (Class II) or do not (Class I) fall under the NIS2 Directive. As the COVID pandemic has shown, some products that may not have been considered critical pre-pandemic, such as on-line conferencing facilities, can rapidly become so. Furthermore, a mechanism for revisiting Class I and II product categories in a timely manner needs to be identified to permit effective cyber surveillance. Such a mechanism may prove particularly important as developments in emerging technologies challenge existing norms of security and encryption standards, and related disclosure and maintenance practices.

Article 10
The requirements of this Article apply for the lifetime of a product or five years, whichever is shorter. This timespan should be harmonised with other proposed legislation, such as the forthcoming right-to-repair legislation (still in the proposal stage), which is intended to enhance the current EcoDesign regime[3]. Adoption of such legislation may result in a mandate that spare parts for several electronic product categories (*e.g.*, refrigerators, home televisions, and electronic displays which now routinely incorporate digital elements) be available beyond the two years currently stipulated by law.[4]

Further, in the event that product lifetimes are extended through the right-to-repair legislation, procedures governing how vulnerabilities related to spare parts (which may be manufactured by third parties) will need to be identified. Similarly, an approach to the recall of hardware products containing covered spare parts also will need to be delineated. In addition to products which have had their lifetime extended through the right-to-repair legislation (if/when it becomes operational), orphaned hardware (currently not covered by the proposed Class I and II lists) should be considered as a special category of identified product, possibly in modified form.

We also recommend that the rules regarding hardware products that rely on white-labelling or white-boxing hardware manufactured or assembled (both within and outside the EU) be clarified. Such rules should address white-labelled or white-boxed hardware whose producers license existing or legacy brand-names for commercial purposes.[5]

---

[3] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698869/EPRS_BRI(2022)698869_EN.pdf

[4] Some experts have argued that the availability of spare parts be mandated for 7-10 years but this timespan has not (yet) been formally proposed in the Commission's right-to-repair legislation.

[5] The most notable example of this kind of licensing in the European context are Nokia phones. Nokia mobile phones are now made by another Finnish company, HMD Global Oy, which licenses the Nokia brand. The question here is what if a well-known European brand with a legacy of instant consumer/business recognition is licensed to a company based in a nation or region with which the European Union is experiencing geopolitical tension?

We note that software bills of material will be central to the successful implementation of the proposed regulations. While we recognize that their detailed form will be dictated in subsequent implementing legislation, Europe TPC nonetheless recommends that the Act define and set forth in general terms minimum standards for what they must contain, consistent with current international standards.

Article 11
It is likely that events will occur at the national level and thus can be shared directly with other national agencies through the EU-CyCLONe, in addition to notifying ENISA.

Article 29
Given the generally acknowledged cybersecurity skills "gap," Europe TPC notes the distinct possibility that the cadre of expert assessors called for by the Cyber Resilience Act may be difficult to recruit in sufficient numbers. Accordingly, it may be prudent and productive in this Article to reference ENISA's "European Cybersecurity Skills Framework (ECSF)."[6] It may be prudent and productive to reference the Framework in this Article and to clarify how the proposed assessors fit within it.

Article 53 Penalties
The description of penalties applicable to infringements by economic operators is currently identified in terms of either a specific monetary cost or percentages of global revenue, whichever is higher. A mechanism for periodically revising the monetary costs and percentage thresholds currently specified should be identified that takes global trends, market activity (*e.g.*, consolidation amongst economic operators), and the prospect of economic operators exercising significant market power into account. Provisions could be made, for example, for re-assessing these thresholds in exceptional circumstances that pose existential (political or economic) risks to either the EU or its Member States. Such risks would need to be defined in a consistent, measured, and proportionate manner.

Annexes
Europe TPC welcomes the inclusion of vulnerability handling requirements in Annex I, but strongly recommends that the Commission also provide guidance on related reporting standards and timelines.

CONCLUSION

ACM's Europe Technology Policy Committee stands ready to leverage the expertise of its thousands of European members to assist the European Commission in its further consideration of cyber resilience in this proceeding, or otherwise with respect to technical matters implicating any aspect of computing and its societal impacts. To request such technical, apolitical input please contact ACM's Director of Global Policy & Public Affairs, Adam Eisgrau, at acmpo@acm.org or +1 202.580.6555.

[6]See *Building a Cybersecurity Workforce* (21 September 2022) https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf