Cybersecurity Coalition

May 25, 2022

Submitted via online consultation tool

Directorate-General for Communications Networks, Content and Technology
Unit H2 for Cybersecurity and Digital Privacy Policy
European Commission

Re: Cyber Resilience Act: Regulation on horizontal cybersecurity requirements for digital products and ancillary services

The Cybersecurity Coalition ("the Coalition") submits these comments in response to the open consultation launched by the European Commission Directorate-General for Communications Networks, Content and Technology on the *Cyber Resilience Act: Regulation on horizontal cybersecurity requirements for digital products and ancillary services* ("the Act"). The Coalition appreciates the opportunity to comment on the call for evidence[1] and looks forward to working with the European Commission on the development of this initiative.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services. 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 has worked with more than 20 governments around the world on the development of national cybersecurity policies, many of which were designed to address issues that are raised in the proposed Act. We are acutely aware of the need to effectively target the supply chain security, as well as to develop products and services with an end-user-centric approach.

The Coalition respectfully offers the following considerations:

The objectives and policy options outlined in the Call for Evidence are too broad. The Coalition acknowledges the importance of the objectives outlined in the document but urges the European Commission to tailor the objectives, and accompanying policy options, to appropriately support the policy goals. As it is written, it is unclear to the Coalition what the core focus of the proposed Act is. Is the proposed Act, for example, focused on supply chain, consumer Internet of Things (IoT) products, or any device connected to the internet? For the Coalition to appropriately provide operational and security recommendations, the scope of the proposed Act needs to be clearer, and narrowly, defined. As such, of the five policy options proposed, we would opt for option 4 which allows for a tiered approach so that scarce cyber

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en

resources can be focused on priority challenges as opposed to trying to tackle, seemingly, everything in one Act.

As written, it is unclear what problem the future Cyber Resilience Act aims to address. The Coalition recognizes that although cyber incidents could be harmful to any organization, there is a lack of technical and independent evidence to assess that "one product can affect an entire organization or a whole supply chain." In fact, most publicly reported cyber incidents are a combination of poor information security practices, failures to appropriately update in a timely manner, individual error, and even malfeasance. Moreover, the document states that "the lack of appropriate security in digital products and ancillary services is one of the main avenues for successful attacks," without mentioning other major sources of attacks, and without providing data regarding that statement.

Furthermore, the Call for Evidence document appears to assume that "vendors" do not put in place adequate cybersecurity safeguards when placing digital products or services on the market and justifies this untrue statement by listing a variety of reasons that are not supported with market evidence. Similar statements are made about vendors' responses to vulnerabilities or responses to product security. The proposed Act provides the opportunity to provide common baseline requirements for safeguards and vulnerabilities across several overlapping pieces of regulation - such as the General Product Safety Directive and the Machinery Directive. Similarly, the recently delegated act for Radio Equipment Directive would also be an example where such additional requirements can be repealed and signposted to those requirements within the future Act. The Coalition recommends that the European Commission explores engaging these existing efforts and measuring their impact, as well as the RED applicable security and privacy provisions, to ensure the current effort promotes a coherent approach to security, rather than starting new and potentially duplicative efforts.

The proposed Act will overlap, and possibly duplicate and disrupt, ongoing security efforts. The Coalition recognizes that although the EU has the legal foundation to work on these issues, the European Commission should consider the practical need for this work and ensure alignment with existing and ongoing initiatives. There is a clear potential overlap between the future CRA, the Directive on security of network and information systems (NIS Directive 2016/1148)[2], and the Radio Equipment Directive (RED)[3], as well as with other worldwide recognized standards such as the Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components (ISA/IEC 62443)[4], and the Cybersecurity, IoT security, and privacy: Device baseline requirements (ISO/IEC DIS 27402). [5]

[2] https://op.europa.eu/en/publication-detail/-/publication/d2912aca-4d75-11e6-89bd-01aa75ed71a1/language-en
[3] https://ec.europa.eu/growth/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en
[4] https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c
[5] https://www.iso.org/standard/80136.html

Cybersecurity Coalition

Fragmentation only decreases security, and a unified approach will help the European Commission accomplish its goal of increasing security.

The Coalition respectfully recommends the European Commission ensures harmonisation across the existing legislations covering cybersecurity of connected products. The proposed Act is an opportunity to embrace and streamline existing efforts, under a single horizontal framework. We also call for a gradual approach to implementation of policy mechanisms to ensure timely evaluation of the impact of a particular set requirement on the market, before introducing a new one.

The Coalition respectfully recommends that the "Act" should focus on creating a baseline of security standards for Consumer Internet of Things (CIoT). The European Commission, Member States, and EU citizens can benefit from existing international- recognized standards such as ISO/EC DIS 27402, ETSI EN 303 645[6], that could serve as guidance frameworks for the development of this initiative. Out of existing, and in development, legislation, there is a policy gap in CIoT security standards which can be filled by the future CRA. If this path is taken, the Coalition also recommends devices be defined clearly, as finished products that connect directly to the internet, in a manner consistent with these standards. It is key the CRA takes into account risk-based approaches to define the security capabilities, allowing for more robust protection to be provided for high-risk environments (e.g. CI, B2B), under other better suited measures (such as the NIS 2.0).

The use of harmonised standard – as governed by the EU's New Legislative Framework - provides a well-established approach to ensure that legislation keeps pace with developing technologies and approaches. It is critical that harmonised standards developed within the CRA must not conflict with international cyber security standards (e.g. ISO/IEC 27001, ETSI EN 303 645, ISO/IEC 29147 etc). Similarly, as enshrined in EU regulation 1025/2012, this future Act should also recognise the ever-growing role of Global fora/consortia[7] (e.g. Oasis, W3C, IETF etc) with regards to developing open standards and technical specifications as well as the ever growing collaboration and relationship[8] between formal Standards Organisations (ISO/IEC and ESOs).

Include input from the Call for Evidence when drafting the proposed CRA text in addition to findings from the study. *The Exploratory Study on the need of cybersecurity requirements for ICT products*[9] only involved 214 participants and 52 semi-structured

[6] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
[7] Page 29 of Digital Europe's Industry Paper: https://www.digitaleurope.org/wp/wp-content/uploads/2020/02/DigitalEurope-A-Stronger-Digital-Industrial-Europe.pdf

[8] The Relationship Between Open Source Software and Standard Setting (2019): https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/relationship-between-open-source-software-and-standard-setting

[9] https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products

interviews, which could be considered an insufficient amount of evidence to serve as the foundation for the development of an initiative that could have significant implications on the security, economic, social, environmental aspects, and fundamental rights of European citizens. We hope that the Commission considers the public comments received during the Call for Evidence with an equal weight as the findings from the interviews, as the Call for Evidence responses will be representative of a variety of sectors and organizations.

The Coalition appreciates the opportunity to participate in this consultation and expresses its availability to work with the European Commission, and other relevant stakeholders, on a deeper analysis of the convenience and benefits that such an initiative would bring to the European community.

Respectfully Submitted,

The Cybersecurity Coalition

CC: Ari Schwartz, Venable LLP
Alexander Botting, Venable LLP
Belisario Contreras, Venable LLP