ITI Submission on the Call for Evidence and Public Consultation of the Cyber Resilience Act

May 25, 2022

ITI - The Information Technology Industry Council appreciates the opportunity to submit comments to the European Commission on the Cyber Resilience Act consultation. ITI is the premier global advocate for technology, representing the world’s most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

We welcome the opportunity for industry to provide feedback. ITI and its members strongly believe that the EU’s efforts to improve cybersecurity resilience across all key economic sectors is foundational to achieving its ambitious digitalisation goals. In doing so, however, it is imperative that regulatory measures adopt a phased and flexible approach, with the ability to adjust regulation as the threat landscape evolves. We stand ready to support these efforts, including by providing our response to the Cyber Resilience Act (CRA) call for evidence.

Below, we share some thoughts around how to improve cybersecurity across the EU and protect digital products and ancillary services across Europe while aligning with and progressing further from existing cybersecurity legislation such as the Cybersecurity Act, the General Product Safety Directive, the Machinery Directive, the Radio Equipment Directive, the proposal for an AI Act, and the NIS2 Directive.

Take A Horizontal Phased Approach That Avoids Fragmentation and Duplication

ITI appreciates the Commission’s continued efforts to improve cybersecurity, including opening a consultation on a proposed horizontal regulatory intervention introducing a common set of cybersecurity rules for digital products and related services. We believe that increasing transparency and advancing product and software secure development practices will indeed strengthen the entire cybersecurity system. However, in order to do so the CRA should be able to overrule existing national legislation covering digital products and ancillary services. The CRA offers the EU an opportunity to take a “precision” regulatory approach, in which regulation is risk-based, includes clear, harmonized rules, is aligned with internationally recognized standards, and avoids overly prescriptive requirements and inconsistencies with other EU legislation. In order to achieve such an approach, the EU must ensure coherence and conformity with existing – and planned – EU legislation, such as the General Product Safety Directive, the Machinery Directive, the Radio Equipment Directive, or the proposed AI Act, NIS2, the Ecodesign Regulation for Smartphone and Tablets, or even the expected Cybersecurity Act’s Implementation for EU wide cybersecurity certification on cloud services, 5G, and IoT and related emerging technologies.

In order to strike a sound balance between potentially competing requirements in forthcoming proposals and existing legislation, the EU European Commission should seek to reduce regulatory divergence. For instance, the provisions on software updates in the Eco-Design Regulation for Smartphones and Tablets mandate that consumers be entitled to roll back security updates and install software updates of their choice. This seems to be in direct contradiction with the objectives of the CRA to put in place adequate cybersecurity safeguards and maintain an appropriate level of security in digital products and ancillary services. A more appropriate approach would be providing...
transparency (to users) on the estimated duration of available update support (while maintaining flexibility to determine that duration and adjust it).

ITI also has questions about how the CRA will interact with provisions stemming from the implementation of the 2019 Cybersecurity Act and the future implementation of article 21 of the NIS2 Directive concerning cybersecurity certification. The objective of the EU Cybersecurity Act is to create an EU-wide framework for voluntary cybersecurity certification of ICT products, services, and processes. We therefore consider it important to ensure that the CRA will not conflict with ongoing implementation efforts related to that Act. In particular, double certification should be avoided, e.g., by making use of the bridge provided for in the Cybersecurity Act, Article 54.3 allowing for, when appropriate, the consideration of certification schemes as an alternative to harmonized European standards when conducting conformity assessment analysis. Yet, certification schemes should not be made mandatory nor replace harmonized European standards. As such, we encourage the Commission to undertake a gap analysis (with stakeholders’ input) of existing and forthcoming legislation in order to pinpoint where additional authorities may be needed to address issues related to cybersecurity.

Next to this, ITI notes that is important that the CRA takes a holistic approach, addressing scope, requirements and conformity assessment all together. However at the same time, the CRA should also recognize that the cyber landscape is constantly evolving and changing, and so should seek to solve challenges iteratively, further developing and improving approaches as the rollout progresses.

One way we believe the EU can establish greater cybersecurity is by improving internal cooperation between the Directorates-General responsible for cyber and related policies. This could be done via standing up an interdisciplinary board or council that discusses EU cyber policy requirements and ensures harmonization. Such cooperation would help tackle policy silos and inject security considerations into discussions across the policy spectrum (e.g. on Ecodesign) as well as balance equities between sustainability, usability and cybersecurity.

Another way to streamline and strengthen cybersecurity requirements is by complementing the CRA with an EU-driven advertising campaign aimed at making people aware of the minimum security standards that the EU is trying to achieve. Cybersecurity awareness programs to make users aware of how to secure their devices are key. Further to this, creating greater awareness on the importance of these security requirements in products will result in customers considering key security criterion when making purchasing decisions (i.e., in addition to desirability, functionality, attractiveness, and costs).

Ensure a Clear Scope and Take a Risk-Based, Phased Approach
ITI supports the Commission’s objective of enhancing and ensuring a consistent high level of cybersecurity of digital products and ancillary services. In order to do so and to avoid confusion, the CRA must encompass a clear scope and definitions, taking into account differences in the development, functionality and use of digital products. One example surfacing already is to clarify what is meant with ‘ancillary services’. ITI also recommends including a clearly scoped definition of a “connected product”, which should be defined as a finished product that is intended to communicate directly or indirectly over the internet. It should also take a proportionate, risk-based approach (e.g. assessing risks in B2C vs. B2B products; embedded vs. non-embedded software). To elaborate, the risk associated with a particular product or service may vary significantly depending on the ultimate use of the product or service. However, we caution the EU against designating entire sectors as high-risk – a thorough risk assessment is
required to understand the threats facing a particular product within a specific sector and further, understand what controls might be needed to mitigate such risks.

As mentioned directly above, the requirements established for products and services in scope should be tailored to mitigate the risk that they might pose when put into service by reducing the impact or likelihood of those occurrences. Taking a risk-based approach to determining the scope of the regulation will also help to ensure that requirements are appropriately targeted at those applications that pose the highest risk and provide a consistent mechanism that balances scope and cost.

As devices become more complex and integrated with other systems and emerging technologies drive new service models, it will be essential that the CRA provides a regulatory framework that is future-proof and adaptable to emerging technologies and offer variations in implementation. As such, ITI strongly urges EU policymakers to focus on the preferred outcomes of such a future framework rather than prescribing specific implementations. This will help industry to grow and remain innovative while reducing the risk of the CRA requirements becoming obsolete over time. Moreover, scoping all three product types (software, services, and physical devices) in parallel prompts challenges with ensuring coordinated and consistent approaches to requirements and conformity assessment methods.

Further to this, we recommend the Commission to consider a tiered approach of sorts, where there is both an ecosystem-wide approach aimed at improving basic security as well as a more specifically targeted set of regulations for products/services deemed high-risk based on a comprehensive risk assessment, which includes an assessment of the end-use of the product or service. Security needs to be proportionate to the risk and to the type of user. In establishing this tiered approach, we encourage the Commission to leverage internationally recognized assurance standards (e.g. ISO/IEC 27402 (in DIS) to establish a cybersecurity baseline for low-risk products, which will create an appropriate foundation from which additional layers may be added for higher-risk products and services. Instituting initial baseline security practices at the finished connected product level, prior to establishing regulation for high-risk products will allow the government to assess the impact of such baseline standards on the cybersecurity landscape, address existing concerns, foresee emerging trends, and effectively tailor solutions using the evidence and foresight provided by that initial phase.

Seek to Align with Industry-Driven Global Standards

As the CRA is further developed, ITI believes that forthcoming rules including harmonized European standards that are based on requirements such as conformity self-assessment by default (including the possibility to have third party assessments for a certain end-use of products/services which can be deemed high-risk) would be an appropriate policy option. In case the CRA proposes more stringent regulation, then we call on the Commission to closely look at comparable policy instruments, such as EU Cybersecurity Certification and how it implements the different levels of assurance following both self-assessments and public cybersecurity certification authorities.

Furthermore, in order to limit fragmentation, ITI cautions against developing ad-hoc regulatory rules. We believe that European standards should be aligned with international standards and vice versa, as international standards provide widely vetted, consensus-based information and guidance for defining and implementing effective security methodologies, and facilitate common approaches to common challenges, thus enabling collaboration and interoperability. In other words, relying on voluntary industry-driven consensus-based international standards and ensuring alignment on base standards are fundamental elements to avoid regulatory fragmentation.
To illustrate, ETSI EN 303 645 ([Cyber Security for Consumer Internet of Things: Baseline Requirements](https://www.etsi.org/deliver/etsi_en/030300_030700/en_303645v01_00.zip)), the NISTIR 8259 Series, and the ongoing development of ISO/IEC 27402.2 ([Cybersecurity – IoT security and privacy – Device baseline requirements](https://www.iso.org/standard/74667.html)) are reflective of such efforts to harmonize global IoT security standards. The former, ETSI EN 303 645 was leveraged as part of the mutual recognition of the cybersecurity labelling schemes between Singapore and Finland. We also want to draw attention to the existing and in-development standards and best practices for software security, including the ISO/IEC 27034 series ([Information technology – Security techniques – Application Security](https://www.iso.org/standard/57479.html)), ISO/IEC 29147 and 30111 ([Information technology – Security techniques – Vulnerability disclosure](https://www.iso.org/standard/63943.html) and [Information technology – Security techniques – Vulnerability handling processes](https://www.iso.org/standard/63943.html)), and the NIST Secure Software Development Framework ([SSDF](https://www.itl.nist.gov/ist/8f4/8f42/appsec/ssdf/)).

Lastly, we encourage EU policymakers to work together with industry on ICT standardization within the existing international and European governance structures. As ICT standardization is global by nature, involvement of all stakeholders is important. The EU already has an effective standardization infrastructure (with CEN-CENELEC-JTC 13, ETSI TC Cyber, ETNO, ITU, etc) in place and it will remain critical to continue to closely engage industry in strategic committees for the development of common technical specifications.

**Taking into account the specificities of software and Open-Source**

The CRA should ensure that the specificities of software are reflected in the upcoming proposal, as the context in which a piece of software is used affects its risk profile, and its components vary throughout its development, integration, and use. Modern cloud-enabled applications are based on software running as composable micro services, which are provided and consumable as SaaS (Software as a service) components. In addition, almost all cloud solutions are built on open-source software stacks and leverage these commonly available software building blocks to form hundreds of thousand different applications.

This is why the author of a software component cannot control the environment in which it is executing. More specifically, the component author could design a software for use in one environment, but it might end up being deployed, unbeknownst to the author, in a completely different environment for which it is ill-suited. Additionally, software will be updated many times and the same piece of software may present a different risk depending on which product it applies to (for example a similar SaaS component in a smart coffee machine vs. usage of the same software building block in a medical device). This is also why tools like Software Bill of Materials (SBOM) with overly prescriptive transparency requirements may not be effective for embedded software.

This is especially true in the B2B world, and in the case of Open-Source development platforms, which are key for supporting strategic autonomy and digital sovereignty as the supplier/developer typically has little control over what their business clients/vendors do with the software and might be limited to intervene by contractual agreements. Indeed, the supplier would have no means of knowing which parts of their product software the client had used, modified, or not utilized.

**Introduce a voluntary mixed policy approach**

With regards to the policy options presented by the Commission in the Call for Evidence, ITI believes that the future proposal should focus on the CRA’s fundamental goal, which is to enhance cybersecurity standards for products and services that are placed on the market. As a result, we conclude that policy option 4, which involves a mixed approach, is most suited, provided that, in addition to a horizontal regulatory intervention for a wide variety of tangible products and ancillary services, only soft measures for non-embedded software are considered. To further ensure a smooth implementation of the CRA, industry should also be offered multiple opportunities to
provide public feedback on the CRA’s provisions once they are developed. Furthermore, it is critical to re-emphasize that a phased approach is necessary to guarantee that requirements are reevaluated on an ongoing basis, based on a cost-benefit analysis and proven effective for a limited number of products and ancillary services before being widely scaled. Finally, industry should be given an appropriate amount of time to practice due diligence through incentives, guidance, and to prepare voluntary self-assessment and third-party assessment opportunities.