Position paper

Proposal for a Cyber Resilience Act

January 2023

TIC Council
Rue du Commerce 20-22, 1000 Brussels, Belgium | +32 2 880 21 37
secretariat@tic-council.org | www.tic-council.org
VAT: BE0724881295 | Transparency Register No.: 840667012559
Formerly known as IFIA and CEOC

TIC Council, the global trade association representing independent third-party testing, inspection, and certification (TIC) organisations, welcomes the objectives of the Commission's proposal for a Cyber Resilience Act.

TIC companies provide independent conformity assessment services, ensuring that certified products comply with regulatory requirements and are secure. Therefore, TIC companies play a pivotal role in successfully implementing the text. The introduction of binding baseline requirements for the cybersecurity of products with digital elements is a step towards a more secure cyber ecosystem. TIC Council suggests the following steps for the text to reach its stated aims.

A comprehensive risk-based cybersecurity framework

TIC Council supports the adoption of a preventive approach through a risk-based framework identifying several levels of criticality. However, the current proposal does not provide a transparent methodology for bringing safe and secure products with digital elements to the market based on the risk they carry.

TIC Council urges policymakers to clarify the risk assessment and product classification methods. Currently, the definition of a "critical product", the criteria for classification between Annex III classes I and II, and the definitions of all product categories, are missing or unclear. Due to inadequately defined risk levels, too many products representing critical risks are classified as "default category" or class I.

For instance, the classification of products into classes I and II, which seems to differentiate between consumer and industrial use, is misleading. It creates the false perception that consumer IoT products are less risky, which cannot be guaranteed in an IoT environment. It also does not promote cybersecurity, as the SolarWinds Orion case[1] may illustrate. This cyberattack, which had critical and far-reaching effects, was directly caused by digital products that would fall under class I (network management system[2], among other things). Therefore, some specific products must be recognised as highly critical, especially those with implications for physical safety, data privacy, or potential scalability effects.

In addition, consistency should be ensured between the essential requirements and the corresponding conformity assessment mandated by sectoral legislation and the new Cyber Resilience Act. This applies to digital products for which cybersecurity threats may lead to safety incidents, but which are not covered in other legislation (e.g., Machinery Products Regulation). Special attention should also be paid to high-risk product categories identified in other legislation, such as the upcoming Artificial Intelligence Act or the revised NIS2 Directive.

An independent conformity assessment for critical products

TIC Council supports the long-existing risk-based approach principle with the mandatory involvement of notified bodies for high-risk products. However, TIC Council members are concerned about the proposed Cyber Resilience Act

[1] https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack

[2] European Commission, Cyber Resilience Act proposal, Annex III Class I, 6.

TIC Council
Rue du Commerce 20-22, 1000 Brussels, Belgium | +32 2 880 21 37
secretariat@tic-council.org | www.tic-council.org
VAT: BE0724881295 | Transparency Register No.: 840667012559
Formerly known as IFIA and CEOC

framework favouring first-party assessment for over 90%[3] of the products covered in the scope. This is even more problematic given that "default category" products are not even required to fully comply with existing harmonised standards in order to be presumed in conformity with the Regulation.

Therefore, policymakers are urged to adopt a proportionate framework reflecting that "even hardware and software considered as less critical can facilitate the initial compromise of a device or network" (recital 7) and should be subject to independent conformity assessment. As currently formulated, "default category" and class I products can be placed on the market through a self-assessment by the manufacturer. As a result, independent notified bodies assess only a small part of products with digital elements in the text's scope as they must only be involved for critical class II products.

Thus, TIC Council strongly recommends that all products presenting a critical risk be subject to a conformity assessment procedure involving an independent notified body. Independent certification by TIC companies is the preferred way to enhance the secure development and operation of products with digital elements throughout the supply chain and already in the design phase. As regards low-risk products, the benefit of a presumption of conformity for the manufacturer must always be preceded by the complete application of harmonised standards; otherwise, a third-party conformity assessment body must be involved.

Continuous assessment of products with digital elements

TIC Council supports the implementation of cybersecurity best practices from the design phase of a product (security-by-design) until its end of use or following any substantial modification. Given the dynamic nature of digital products, compliance with baseline cybersecurity requirements of digital products should be assessed on an ongoing basis.

In the TIC industry's view, only more robust and consistent pre-market access rules, such as strong accreditation rules and mandatory independent conformity assessment procedures, will prevent non-compliant and dangerous products from entering the market. However, the manufacturer should be responsible for mandatory lifecycle support as products with digital elements are continuously exposed to risks that need to be addressed and which are not the sole responsibility of the users.

Contact person: Mann Nguyen, Junior Public Affairs Officer

Rue du Commerce 20/22, B-1000 Brussels
tel: +32 490 57 69 54
email: mnguyen@tic-council.org

TIC Council is the global trade federation representing the independent third-party Testing, Inspection and Certification (TIC) industry which brings together about a 100 member companies and organizations from around the world to speak with one voice. Its members provide services across a wide range of sectors: consumer products, security, medical devices, petroleum, mining and metals, food, and agriculture among others. Through the provision of these services, TIC Council members assure that not only regulatory requirements are met, but also that reliability, economic value, and sustainability are enhanced. TIC Council's members are present in more than 160 countries and the wider TIC sector currently employs more than 1 million people across the globe.

[3] European Commission, Cyber Resilience Act factsheet, page 3, September 2022