EU Cybersecurity Act : AmCham EU welcomes improved governance framework but further progress needed

Security certification is a well-established tool that can play a role in increasing resilience and awareness for business users and consumers. The American Chamber of Commerce to the EU (AmCham EU) supports the objective of the European Commission's proposal to reduce administrative costs and ensure there is a stronger and more harmonised approach to cybersecurity certification.

It is in the industry's best interest to incorporate the high levels of security in products and services, baked in through security by design and assured through stringent security standards such as the ISO 27000 series. AmCham EU members typically operate across borders and therefore rely on a variety of security tools, including global standards and international certification processes to ensure the cybersecurity of their products, services and processes. Furthermore, cybersecurity is a responsibility of government and industry alike and the most effective way of advancing it is through public-private partnerships involving open dialogue and trusted collaboration. Under the future EU certification framework, it is therefore of paramount importance that companies maintain the ability to develop the security system features best designed for their unique risk situation.

The governance framework defined in Title III of the EU Cybersecurity Act should promote a market-driven, inclusive and risk-based approach. We welcome the fact that the report adopted by the European Parliament's industry committee improves the legislative text in a number of areas; we urge co-legislators to include further improvements to ensure that the EU certification schemes will be practical for the EU's security needs. Therefore we hope that our comments below will be taken into consideration during the upcoming informal trilogue process:

1. We welcome broadened scope and strengthened industry involvement

We welcome the introduction of new language on a standardised and transparent process for preparing candidate schemes, as well as the broadened scope from products and services to processes (compromise amendment (CA) 8). We strongly welcome that industry involvement in the preparation and adoption of certification schemes is now guaranteed and significantly strengthened thanks to the existence of a Stakeholder Certification Group that will be involved throughout the process of proposing, developing and adopting each candidate scheme also through the setup of ad-hoc committees (CA 11 on Article 20a and Recital 44a and CA 8 on Article 8(a)(1)). We also strongly support the new provisions requiring ENISA to consult with all stakeholders in a formal, open, transparent and inclusive consultation process (CA 13, Article 44(2)).

2. Assurance levels must reflect a risk-based approach

The changes introduced by the industry committee bring some improvements: article 46 a (new) (CA 15) provides a stronger linkage to actual assessment rather than static levels. However, this could be improved by allowing self-assessment for 'substantial' and 'basic' risks as further discussed below. Furthermore, depending on the category, more than three levels of assurance may be appropriate. The ITRE wording on assurance levels (CA 15, article 46) could impose multiple certification requirements, as the European Parliament wants to link the assurance levels to 'the intended use' of the ICT product, process or service. This could lead to a situation where a product with same

American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
amchameu.eu • European Transparency Register: 5265780509-97

More information:
Maika Fohrenbach
mfo@amchameu.eu

functionalities and security features is required to be certified against different criteria (which also seems suggested by the wording in Article 46a (new)). We call on co-legislators to further clarify the role of assurance levels in line with a risk-based approach.

3. Self-assessment of conformity should be possible for 'substantial' risk level

We welcome that the possibility for companies to carry out self-assessment of conformity is explicitly recognised in the committee's position (CA 15, Article 46a (new)), but this should not only be limited for the assurance level 'basic', as this does not reflect the current business practice which covers the categories which could fall under the assurance level 'substantial'. We therefore urge co-legislators to extend the possibility of self-assessment for products falling under this 'substantial' risk level category.

4. Alignment with global practices and strong reliance on international and European standards

The importance of ensuring consistency with international standards and international certification processes (notably in CA 16, article 47) should be further stressed to guarantee alignment with international best practices and standards on not-publicly known cybersecurity vulnerabilities disclosure procedures; we therefore regret the rejection of AM 534 (article 47 (1) (j)). Furthermore, we would like to stress that 'pan-EU security standards harmonisation for IoT devices' (as foreseen in CA 10, article 20) standards should be based on international standards and, if there is a gap, developed through the appropriate standardisation channel.

5. Security objectives need to reflect product realities

Some of the security objectives foreseen in the legislative text can be further improved to reflect the product realities. Companies cannot ensure that ICT products, processes and services do not contain vulnerabilities as they are continually emerging and, in many cases, not known or knowable (article 45 paragraph d) in CA 14). In particular, we recommend updating the language to state 'that ICT products, processes and services do not contain ***known*** vulnerabilities'. This language, coupled with the language in paragraph (e) on processes for dealing with newly discovered vulnerabilities, can best achieve the intended objective. Furthermore, paragraph (h) is very broad and not sufficiently qualified to understand what type of requirements are referred to.

6. Security by design and secure development process-based certification

AmCham EU welcomes the ITRE committee's focus on security by design and certifications based on secure development processes (CA 14 and 16 on articles 45 and 47). Modern software development lifecycles are short and application updates are often issued multiple times in a given year, month, week or even day. Leading development organisations build security into their development processes and make this a mandatory consideration during the development of all software. Certification schemes that focus on secure development processes and practices can help ensure strong security while aligning with modern development approach.

We trust these points will be considered for the on-going negotiations, which we hope will lead to an effective cybersecurity certification framework in Europe.

American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
amchameu.eu • European Transparency Register: 5265780509-97

More information:
Maika Föhrenbach
mfo@amchameu.eu