AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

Cyber Resilience Act

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.4 trillion in 2021, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Introduction

The **American Chamber of Commerce to the European Union** (AmCham EU) supports a strong cybersecurity environment in Europe. As the European Union's economy and society continue to embrace digital solutions, there is an urgent need to ensure that the EU's networks and information systems are resilient against evolving cyberattacks. Cybersecurity is a responsibility of government and industry alike, and the most effective way to strengthen it is through public-private partnerships, harmonisation and global cooperation. In order to make this ecosystem thrive, it is fundamental to make security and trust a priority, and to ensure the security of the entire supply chain is reinforced to avoid security risks in products and services as well as to protect customers and citizens against malpractices and abuse.

The future Cybersecurity Resilience Act (CRA) will address a wide range of digital products and services. This paper outlines key recommendations regarding aspects of the expected CRA that require clarity and focus. Our suggestions encompass the scope, security requirements, the role of the industry, harmonisation, market surveillance, differences between Business-to-Business (B2B) and Business-to-Consumer (B2C) products.

Clarity on scope

The digital or Information and Communications Technology (ICT) products that will be in scope of the CRA need to be clearly defined. It is important to take a holistic approach to address the hardware and software elements of digital products entering the EU market – both on a quantitative and qualitative level.

Effective requirements

The Commission should develop a proportionate approach to develop security requirements based on corresponding product categories, intended use cases and levels of risk. As an instrument to demonstrate conformity, cybersecurity certifications are a strong tool that can ensure harmonisation across the Single Market. However, we advise against mandatory certification and prescriptive requirements in the future regulation, to ensure it remains flexible, future-proof and outcomes-based. To assess the applicability, efficiency and market impact of the requirements, the Commission should also consider using a gradual approach when implementing them.

Industry as stakeholder

There should be continued transparency and engagement with the industry when building the legislative framework and setting the standards and technical requirements for products in scope. Input from the industry will ensure that the requirements address the evolving cybersecurity challenges without hampering innovation.

Need for harmonisation

The CRA is an opportunity to create a horizontal framework that will enhance the cybersecurity resilience of digital products on the EU market. In order to achieve this, it is key to avoid overlapping rules and achieve harmonisation among the existing legislative framework that address conditions for product placement on the market (ie, Delegated Act of the Radio Equipment Directive, Machinery Directive, Ecodesign Directive and New Legislative Framework). To avoid creating additional trade barriers for global companies operating in the EU and European companies operating globally, international standards should be leveraged.

Focus on self-assessment and market surveillance

Self-assessments should be leveraged to reduce the costs of both compliance and supervision with the new legislation. At the same time, it is important to leverage the existing frameworks for market surveillance and compliance.

Consider differences in B2B and B2C products

B2B and B2C digital products (ie, industrial Internet-of-Things [IoT] applications vs. consumer connected devices) have different lifecycles, risks and intended purposes. In a B2B environment, products are integrated into highly complex systems, and such specificities should be considered when defining cybersecurity requirements in the CRA. For example, modern cloud-enabled applications are based on software running as composable micro services that 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 are leveraging these commonly available software building blocks to form hundreds of thousand different applications. This is why a B2B software developer would typically have little control over what a business client does with the software – or how it will be deployed, modified or utilised – and may be even limited to intervene by contract.

Alignment on objectives

It seems that the EU Commission seeks to introduce not only security standards for products and services, but also to address defence aspects (ie, the use of offensive measures in addition to security measures). We urge the Commission to align its different objectives early in the legislative process to ensure an approach that will be beneficial for stakeholders and stakeholder input. Without such alignment, any attempt of regulation will face serious legal issues which will be hard to reconcile once the regulation is adopted.

Fit with existing legal framework

The CRA will complement the existing EU legislative framework, which includes the Directive on the security of Network and Information Systems (NIS Directive),the Cybersecurity Act and the future Directive on measures for high common level of cybersecurity across the Union (NIS 2) that the Commission proposed. It is crucial to make sure that any provisions in the CRA which touch upon rules that are similar to those already existing in other legal frameworks, are properly assessed. In case of overlap or even contradiction, such provisions should be reduced to the minimum necessary based on legal considerations or completely removed to avoid duplication or non-effective requirements. Otherwise, the CRA will not successfully add to the cybersecurity landscape in a positive and meaningful way to protect EU industry and the broader EU society.