U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

Mr. Thierry Breton
Commissioner for Internal Market
European Commission

Ms. Carme Artigas Bruga
State Secretary for Digitalisation and Artificial Intelligence
Ministry of Economic Affairs and Digital Transformation
Government of Spain
Presidency of the Council of the European Union

Mr. Nicola Danti
Rapporteur for the EU Cyber Resilience Act
Renew Europe Group
European Parliament

U.S. Chamber of Commerce Recommendations: EU Cyber Resilience Act Proposal

August 11, 2023

Dear Commissioner Breton, Secretary Bruga, Mr. Danti,

The U.S. Chamber of Commerce ("Chamber") supports the European Commission's efforts to reduce cybersecurity risk in the EU and seeks to serve as a committed partner in this endeavor. We applaud the goals of the EU's forthcoming EU Cyber Resilience Act (CRA) and welcome the opportunity to share our views on principles that should underpin the legislation to ensure it achieves its objectives.

The Chamber is the world's largest business advocacy organization, promoting free enterprise and advancing American trade and investment globally. In Europe, we work closely with our partner organizations at AmCham EU, American Chambers of Commerce in all 27 member states, and with our counterparts at BusinessEurope and other member state business organizations.

We are committed to enhancing cybersecurity throughout the European Union by adhering to a risk-based approach and developing an enhanced baseline for cybersecurity requirements, and we submit the following recommendations for consideration by co-legislators as the CRA enters the trilogue phase in the coming weeks.

U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

Key Recommendations

1. **Clarify the scope of the proposal to exclude cloud-based services:** Greater clarity is needed regarding the scope of covered products and services. Under Article 3(1), a variety of software services are brought into scope when using "remote data processing" language to define a "product with digital elements." Specifically, the article defines "products with digital elements" as "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately." **We recommend that this language be changed so that CRA explicitly state it does not apply to cloud-based services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and open-source software (OSS).**

2. **Align with existing international standards:** The CRA must complement existing cyber legislative initiatives in the EU and globally and align with existing, agreed-upon international norms. The CRA must remain coherent with requirements included in legislation such as the EU Cybersecurity Act, Network and Information Systems Directive (EU) 2022/2555 (NIS2 Directive), Radio Equipment Directive 2014/53, and General Data Protection Regulation (GDPR). Regulatory misalignment will create significant conflict of law scenarios, unnecessarily complicate compliance, and undermine effective cybersecurity outcomes.

NIS2 Alignment: In particular, incident reporting obligations outlined in the CRA proposal need to align with the requirements of NIS2, reducing areas of duplication of efforts for industry and confusion for competent authorities. The CRA proposal should be amended to meet the definition requirements of NIS2, notably that reporting is limited to "confirmed significant" incidents. CRA also should be amended to exclude the reporting of "any incident having an impact on the security of the product with digital elements" to be reported and "any actively exploited vulnerability." We believe it is inappropriate to require industry to disclose actively exploited vulnerabilities that have not matured to an incident, pose a significant risk, or have not yet been mitigated. As currently written, the proposal would include external security research and low-risk vulnerabilities, creating unnecessarily burdensome reporting requirements – for companies and regulators alike.

Including a broader scope for reportable incidents would hinder companies' abilities to counter more active severe threats and risks inundating competent authorities with reports on incidents that do not pose a serious risk, creating noise. Amending the scope of a reportable incident is beneficial for all parties.

Lastly, the proposal suggests mandating that incidents be reported to ENISA, which is inconsistent with the procedures outlined under NIS2 whereby incidents are reported to CSIRTs and national competent authorities. Instead, CRA should build upon previous iterations of cyber policy and recognize the role of competent authorities and national CSIRT networks. We are also concerned

about the Council's amendment to Article 11(4), which permits CSIRTs to share information about vulnerabilities and incidents without a manufacturer's consent when it is deemed that a manufacturer did not inform users "in a timely manner," as we believe this will adversely impact cybersecurity (see June 21, 2023, Joint Industry Statement). **We recommend that CRA adhere to the requirements outlined under NIS2, in which entities report incidents to CSIRTs and national competent authorities.**

GDPR Alignment: The reporting timeline for incidents in the current proposal differs from GDPR, which states that significant incidents should be reported without undue delay in no less than 72 hours. The current CRA proposal of 24 hours needs to be revised and aligned to the global standard of 72 hours. 24 hours does not provide companies with adequate time to assess the severity of an incident and confirm that a significant incident has occurred. It also would undermine companies' ability to counter incidents in progress by taking away valuable resources to meet unreasonable reporting timelines. **The Chamber encourages the global harmonization of incident notification timelines of no less than 72 hours after an affected entity confirms a significant cyber incident.** Doing so will ensure that reporting entities can provide information to the government or the public that is comprehensive, properly contextualized, and as accurate as possible at the time of reporting.

Specific Cybersecurity Standards Alignment (i.e., ISA/IEC 62443, ISO 27000, ISO 27001, and NIST CSF): To promote standards harmonization, the standardization requests of the Commission should consider specific technical international information security standards, notably ISA/IEC 62443, ISO 27000, and ISO 27001. **We recommend mutual recognition where essential requirements align, specifically for the above-mentioned standards. Furthermore, the Chamber supports integrating the standards, guidelines, and best practices to manage cybersecurity risk into the CRA proposal included in the U.S. National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF).**

Finally, essential requirements under the existing CRA proposal, such as free patching and the delivery of products with zero known exploited vulnerabilities, are impractical as currently written.

3. **Include adequate timelines for implementation**. The Chamber encourages co-legislators to extend the implementation period for industry adoption and to permit greater European harmonization of standards.

Article 57 of the current proposal states that all the articles will apply 24 months after the CRA enters into force. This timeline is unrealistic as many products take longer than 24 months to be designed, developed, and deployed. To meet conformity and certification assessments, more time is needed for industry to assist their customers with replacing and updating products, as well as ensuring continued interoperability. **We recommend that the implementation period be amended to 48 months and that consultations with industry occur whenever there are substantial**

changes in policy, security controls, standards, and usage. The experience of the delegated act of the Radio Equipment Directive (where the Commission had to postpone application of the act due to the lack of harmonized standards) offers an important lesson here.

4. Pursue voluntary certification based on risk: Companies should maintain the ability to choose if they wish to certify their product using a European cybersecurity certification scheme or use the conformity assessment procedures of the CRA. Certification is a time-intensive and costly endeavor in which companies should be allowed to pursue voluntary certification based on risk. The Chamber supports the previous statement made in Article 56 of the EU Cybersecurity Act (CSA) that "The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law." For ICT products, services, and processing cybersecurity certification schemes authorized in the EU Cybersecurity Act, the U.S. Chamber urges EU policymakers to support risk-based approaches to certification schemes and ensure that the security objectives avoid digital sovereignty requirements, are aligned with Article 51 of CSA, and are mandatory only in the case of high-risk ICT products, services, and processes.

5. Conformity assessment modifications: In the case of substantial modification, for example, when a security update addresses a known vulnerability or an update to a product with digital elements increases cybersecurity and reduces risk, a new conformity assessment should focus only on aspects affected by the modification.

6. Amend essential requirements and technical documentation: Section 1 of Annex 1 requires companies to place products on the market that do not have any known exploitable vulnerabilities. The Chamber does not believe that this is workable and supports an amendment that considers a risk-based approach. Per Annex V, manufacturers are also still required to include excessive information in the technical documentation despite the clarification that this information must only be made available to market surveillance authorities and not be made public. Lastly, the Council's text includes the possibility for users to "opt-out" from automatic updates, but this language does not provide manufacturers with the flexibility not to provide automatic updates, which we believe is needed in the business to business (B2B) context. The above inconsistencies for essential requirements and administrative procedures must be addressed for industry to operate effectively.

7. Stakeholder engagement is essential: The U.S. Chamber strongly supports multi-stakeholder engagement, including robust public consultation, to inform cybersecurity requirements, rules, and regulations before they are finalized. Our experience has been that consultation with industry has a positive impact on cybersecurity rules and reduces the risk of redundant or consistent approaches that undermine security across jurisdictions, regulatory bodies, and agencies. The Chamber would be pleased to act as a convener for additional stakeholder

engagement sessions, both formally and informally, akin to U.S.-EU Cyber Dialogue we hosted in Washington in December 2022.

8. **Align CRA security objectives with existing EU law:** To remain consistent, CRA should incorporate the same security objectives outlined under the EU Cybersecurity Act (CSA). Under Title III, Article 51 of CSA states that EU states must strive to meet ten specific security objectives. The Chamber supports these security objectives as they are based on sound, technical, consensus, international, and industry-led standards, and we believe they should be included in the CRA proposal as well. The security objectives included in the CSA are as follows:

    (a) to protect stored, transmitted or otherwise processed data against accidental or unauthorized storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;
    (b) to protect stored, transmitted or otherwise processed data against accidental or unauthorized destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;
    (c) that authorized persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
    (d) to identify and document known dependencies and vulnerabilities;
    (e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
    (f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
    (g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;
    (h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;
    (i) that ICT products, ICT services and ICT processes are secure by default and by design;
    (j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

The co-legislators should incorporate the above CSA security objectives in the CRA proposal.

9. **Avoid discriminatory policies that limit secure and trusted ICT product and service providers' access to the European market:** Proposed policies such as the European Cybersecurity Certification Scheme for Cloud Services (EUCS) include ill-thought-out requirements that discriminate against foreign-based companies, and which could in fact undermine EU cybersecurity. Specifically, EUCS prevents non-European-based cloud service

U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

providers from earning certifications at the highest level of security, which may effectively ban these providers from the European market. This form of digital protectionism is not based on sound technical standards, core cybersecurity principles, or best practices.

EUCS would adversely impact European security and resilience at a time when we face unprecedented economic and geopolitical challenges—and when the transatlantic public-private partnership has proven essential to protecting cybersecurity in Ukraine and beyond.

It is widely understood that cloud computing confers significant security benefits over on-premises infrastructure, as it simplifies the task of continuously monitoring for threats and vulnerabilities. Global cloud infrastructures provide superior resilience if natural disasters or armed conflicts threaten local data facilities or networks. Data localization requirements lead to higher costs for businesses and consumers and pose significant liabilities from a security and resilience perspective.

Therefore, we urge the co-legislators to omit the discriminatory policies outlined in EUCS and refrain from including such policies in future legislation. Discriminatory factors such as the location of a company's headquarters or the nationalities represented on its board should not be used as a proxy for trustworthiness. Instead, the EU should prioritize a risk-based approach that considers company practices and the data-sharing requirements that may apply to state-owned enterprises or companies headquartered in authoritarian countries.

Conclusion

The Chamber is firmly committed to the cybersecurity and economic vitality of Europe. We welcome the opportunity to discuss these recommendations further and look forward to working closely with EU policymakers as the Cyber Resilience Act moves forward. Thank you for your consideration of our views.

Sincerely,

Marjorie Chorlins

Marjorie Chorlins
Senior Vice President, Europe
U.S. Chamber of Commerce

Vincent M Voci

Vince Voci
Vice President, Cyber Policy and Operations
U.S. Chamber of Commerce