AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

European Commission Cybersecurity Act consultation

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 €4 trillion in 2023, directly supports more than 4.6 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 56, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive summary

- ENISA should have more resources available to reflect its growing role in the EU cybersecurity ecosystem and to support implementation of new cybersecurity legislation like NIS2, CRA, DORA.
- EU certification frameworks should draw from international standards to ensure a quicker and broader market uptake of the schemes as well as a more efficient certification development process.
- The Cybersecurity Act (CSA) should incorporate a more active role of industry in the certification development process.
- CSA should remain a technical framework for a transparent, inclusive and evidence-based certification development process.
- Simplification of cybersecurity legislation is a key priority and should ensure that the compliance and reporting burden faced by companies is appropriately calibrated. More specifically, we recommend to:
    - Clarify the scope overlaps between NIS2, DORA and CRA to provide legal certainty, especially for entities such as cloud service providers.
    - Align reporting obligations by leveraging national single reporting entry points and clearer reporting thresholds.
    - Simplify conformity assessment process across cybersecurity legislation through uniform assessment methodologies and mutual recognition of assessment results across Member States and conformity assessment bodies (CABs).
    - Align and leverage one-stop-shop approach across cybersecurity legislation.
    - Clarify the application of “substantial modification” for software under the New Legislative Framework (NLF).
- Supply chain security policy should be risk-based and technical, avoiding non-technical or discriminatory assessment criteria.

Introduction

AmCham EU represents the interests of American companies operating in Europe, spanning a wide range of sectors including technology, finance, manufacturing and services. Our members are committed to supporting the EU’s efforts to strengthen cybersecurity and digital resilience across the Single Market. This position paper outlines the collective views of US companies on the ongoing review of the EU Cybersecurity Act, with the aim of ensuring that future policies foster innovation, facilitate transatlantic trade and provide effective protection against evolving cyber threats.

US companies are supporters of strong cybersecurity frameworks and recognise the EU’s leadership in this area. As the European Commission considers revisions to the Cybersecurity Act, it is essential

that the regulatory environment remains open, balanced and globally interoperable. The Commission should adopt a risk-based, proportionate approach to certification, ensure meaningful stakeholder engagement and avoid the creation of unnecessary barriers to market entry. By aligning with international standards and recognising existing certifications, the EU can enhance security while supporting innovation and economic growth.

US companies share the EU's commitment to enhancing cybersecurity and protecting digital infrastructure, investing heavily in security measures and working closely with European partners to address emerging threats. A strong, harmonised cybersecurity framework is vital for the resilience of the digital economy and the protection of consumers.

1. Mandate of ENISA

Since 2019, the EU's legislative framework for cybersecurity has evolved, delegating ENISA new tasks and strengthening its position in the EU cybersecurity ecosystem. Therefore, ENISA's resources need to be re-assessed. In the light of the ongoing transposition of NIS2, the publication of the CRA and the new Cyber Solidarity Act, ENISA needs additional (rather than re-allocated) resources to be able to fulfil its mandate without deprioritising other activities, such as timely and efficient development of certification schemes. Taking into account the updated EU cybersecurity policy landscape and ENISA's role in it, we propose specific recommendations on amending the Agency's mandate below.

Reinforce ENISA's role as an independent agency on EU cybersecurity and enhance cooperation with international partners

It is important that the reviewed CSA supports ENISA's capacity to operate independently and attract the necessary resources, staff and experts to carry out its mandate effectively. ENISA should leverage its public standing among the global community and be empowered to develop and implement international projects and programmes with partners such as the US Cybersecurity and Infrastructure Security Agency (CISA) or the UK's National Cyber Security Centre (NCSC). Further international harmonisation and engagement could aid ENISA's objectives, including – for example - ensuring consistent post-quantum cryptography timelines. ENISA should also have the autonomy to cooperate with industry experts and businesses, irrespective of their country of origin or main establishment**.** Private sector partners could bring critical threat intelligence, operational expertise and technological innovation that complement ENISA's mission. ENISA's autonomy and freedom to cooperate with industry experts and businesses should be ensured, irrespective of their country of origin or main establishment.

Clarify ENISA's role within the complex EU institutional landscape

Following the implementation of the Regulation to establish common cybersecurity measures across European Union institutions, bodies, offices and agencies, the cybersecurity ecosystem of the EU will grow more complex. Alongside ENISA and the European Cybersecurity Competence Center (ECCC), CERT-EU will receive a strengthened mandate. Although the roles and mandates differ, undoubtedly it creates complexity and the potential for confusion. This will impact the role and the effectiveness of independent agencies such as ENISA. The Commission should clarify the different roles, responsibilities and mandates of CERT EU, ENISA and ECCC.

Improve and deepen strategic stakeholder engagement

Experts and private sector representatives could bring more evidence and support to ENISA's activities. Engagement should prioritise structural cooperation that includes the entities in scope of EU Cybersecurity regulation and initiatives (NIS2, CRA, DORA, Certification schemes).

ENISA should dedicate resources (a strategic unit) to manage public-private stakeholder engagement in order to better leverage knowledge and expertise of the wider cybersecurity community. This unit would be responsible for managing its stakeholders at a strategic level, to ensure ENISA is inclusive and transparent, and to push forward innovation of the existing Working Groups into bodies that provide added value to the Agency and European cybersecurity.

Leverage ENISA's expertise in policy development

ENISA should expand its policy engagement capacity, operating with increased autonomy and sharing technical expertise as well as guidance to support cybersecurity policy development. This should be achieved by investing in and establishing relationships with the 27 EU Member States regulators and policymakers as well as with the European Parliament and Council.

ENISA should also develop an independent European Cybersecurity Policy Development Radar with a span of 3 to 5 years that shall guide the Agency's activities. Stakeholders should be consulted for input and discuss cooperation through a formal Stakeholder Policy Group that includes both public and private partners and is chaired by ENISA.

Enhance cybersecurity skills development

In parallel, to further strengthen the implementation of EU cybersecurity policies, it is essential that ENISA is granted additional resources to address the critical area of cybersecurity skills development. The European Cybersecurity Skills Challenge stands out as one of the EU's most successful initiatives in this field, demonstrating real impact and fostering a new generation of cybersecurity professionals.

However, despite its broad reach and impact, the programme currently operates with insufficient funding. Expanding financial support would enable increased cybersecurity training opportunities - such as through accessible online platforms - and help cover essential travel expenses for participants from all member states to join the final Capture the Flag (CTF) competition, thereby maximizing the initiative's potential to benefit the entire European cybersecurity community.

2. European Cybersecurity Certification Framework

2.1. More effective certification development

The intent of the Cybersecurity Act's (CSA) original text was to provide a framework for the development of harmonised certification that would improve users' trust and serve market needs. For

example, according to Recital 69 of the CSA, the EU-level schemes should reduce cost for undertakings operating in the EU. According to this recital, the schemes must also be non-discriminatory. Indeed, the Cybersecurity Act should not create de facto barriers to entry for non-EU products and services. Requirements that are overly restrictive or not aligned with international practices could limit consumer choice, reduce competition and hinder the availability of innovative solutions in the EU market. Fair competition and open markets are essential for driving investment and technological advancement.

More specifically, the sovereignty-related requirements that have been under discussion for the EU Cloud Certification Scheme (EUCS) are either difficult or impossible to meet for providers coming from outside of the EU. This also leads to higher costs for providers and for users, not least due to distorted competition. AmCham EU supports a Certification Framework that produces **technical, standards-based schemes achieved through open consultations**. This approach will serve the interests of businesses, citizens and the European economy as a whole and speed up the approval process. Any review of the Certification Framework must refrain from including non-technical measures, such as sovereignty requirements, which will only raise costs, limit choice for European users and hinder European competitiveness.

Additionally, the **structure and governance of the ECCG and SCCG should undergo review** to ensure that the processes of certification development and adoption are sufficiently separated. The Commission's role is to develop Implementing Acts for certification, thus it should not be involved in the development (technical) phase. For this reason, the Commission should not be the chair of the ECCG, a role which could be changed to follow Council Presidency rotation. In addition, The SCCG chair role should be handed over to ENISA.

Certification requirements should also be tailored to the level of risk associated with specific products and services. A one-size-fits-all approach could stifle innovation, particularly for small and medium-sized enterprises (SMEs) and emerging technologies. The Act should provide flexibility for companies to demonstrate compliance in ways that are appropriate to their risk profile and business model.

Finally, **the Commission must establish a clear precedence of European certification schemes** over national schemes according to Recital 94, 98 and Art 57 (1) of the CSA. The key goal of EU certification framework is to bring harmonisation across the EU Member States.

2.2. The role of industry

The Commission should create a transparent and inclusive consultation process for the cybersecurity certification framework in line with the objectives of Recital 83 and Art 49 (3) of the Cybersecurity Act (CSA). There should be a clear mechanism for industry input since existing platforms like Stakeholder Cybersecurity Certification Group (SCCG) do not fulfil this function and have proved insufficient to ensure transparency of the certification development process. For example, Recital 62 outlines SCCG's role in ensuring consultation process with relevant stakeholders – however, so far, the communication between ENISA and SCCG has clearly been organised in a one-way manner. The SCCG should gain a more tangible role within the certification preparation and development process in contrast to what is currently expected from it in Article 22. New frameworks must envisage industry stakeholders' mandate to consult, advise and provide feedback, opinions and assessments to ENISA as well as

support market impact assessments related to draft certification schemes. Moreover, European Cybersecurity Certification Group should meet with the SCCG – or a new stakeholder consultation group – on a regular basis to discuss progress and technical issues related to certification schemes.

Stakeholders must also be able to provide direct input to existing networks like the CSIRTs Network or the NIS Cooperation Group. This will ensure that ENISA and national cyber authorities have input from industry before decisions are made. ENISA should devote additional resources – for example, a full unit – to public private cooperation.

2.3 Assurance levels

The Commission or ENISA must **clarify the methodology** for allocating workloads into different assurance levels. Article 52 of the CSA does not provide any guidance on how assurance levels are assigned as well as who assesses which specific data must fall under a specific assurance level. Such clarity is essential during the development of the schemes to understand the level of security and type of controls that must be deployed for respective assurance levels.

2.4 Union Rolling Work Programme

The Union Rolling Work Programme (URWP) should be developed as a tool to guide industry to prepare for the future certification. Therefore, URWP must be **regularly revised in an open, transparent and collaborative manner** which incorporates market needs. To ensure such a process, AmCham EU recommends including industry consultation as a prerequisite to updating the Union Rolling Work Program (URWP):

*'inclusion of specific ICT products, ICT services and ICT processes or categories thereof, or of managed security services, in the Union rolling work programme **shall follow a public consultation** and shall be justified on the basis of one or more of the following grounds'*

Transparency of both drafting and revision process should be improved with the involvement of wider industry in a consultation process, which is not currently clearly included in Art 47 of the CSA.

2.5. International alignment

Where possible, the EU **should recognise or align with existing international certifications and schemes**. Mutual recognition and equivalence agreements can help facilitate cross-border trade, reduce duplication, lower compliance costs, prevent market fragmentation and accelerate the adoption of secure technologies. This approach will benefit both European and international companies, as well as end users.

Draft schemes produced so far often lacked reference to international standards, such as those developed by International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC) JTC1 SC27 (ISO/IEC 27000 series), leading to ambiguous terminology and requirements not grounded in industry best practices and standards. Any updates to the Certification

Framework must ensure that it leverages existing international standards to the fullest extent possible.

3. Simplification of cybersecurity and incident reporting obligations

3.1. Scope and overall alignment

The definition of '**remote data processing services'** should be further clarified to avoid legal uncertainty and overlaps in the scope of CRA and NIS2. Providers of cloud solutions appear to be excluded from the CRA but are then brought back into the regulation if they offer applications, which in today's mobile-first world, is often a requirement. This overlap duplicates requirements for cloud solutions providers, making compliance with both the NIS2 and CRA requirements complex and costly, likely hindering the emergence of European cloud providers. Accordingly, **providers of cloud solutions that are in scope of NIS2 should be explicitly and fully excluded from the CRA**.

The financial sector is subject to sector-specific regulation and has an existing cybersecurity and operational resilience framework under the Digital Operational Resilience Act (DORA). DORA applies to the end-to-end IT infrastructure of financial entities. The CRA therefore applies a duplicative framework, with the same policy objectives, to financial sector applications that are in-scope of DORA. Product legislation should not apply to financial services as there remains significant uncertainty within the sector concerning how enforcement will occur in practice, how product terminology is interpreted for intangible services and how applications relate to the underlying financial services being provided. AmCham EU encourages the removal of the financial sector from scope via a Delegated Act in Article 2(5).

3.2. Conformity

The harmonisation goal of NIS2 is challenged by additional national rules and varying conformity assessment processes required nationally. To address this, the EU should establish a centralised conformity assessment framework, ensuring that all cybersecurity legislation follows **uniform assessment methodologies and mutual recognition** of certifications across Member States.

Conformity Assessment Bodies (CABs) should be aligned so manufacturers can ideally use a single CAB per product, inclusive of all relevant cybersecurity legislative requirements.

Manufacturers facing multiple cybersecurity regulations may have to engage with different CABs for each regulatory requirement. Policymakers should allow and encourage one conformity assessment body to cover all relevant cybersecurity certifications for a product. Concretely, this could mean expanding the scope of accreditation for CABs: organisations that are qualified to assess under the CRA should also be able to seek designation under the AI Act (and vice versa), creating a pool of 'multi-regulation' cybersecurity CABs.

In addition, mutual recognition of test results between CABs should be institutionalised. If one CAB has already tested key technical aspect, such as encryption or vulnerability management, other CABs should accept those results and focus only on regulation-specific requirements. This approach maintains high assurance levels while reducing redundant testing and cost.

3.3. Reporting

To make cybersecurity reporting simpler, businesses should be subject to a single reporting regime whereby they report incidents under one format, to one EU entity.

Inconsistent cybersecurity reporting requirements result in:

- Companies drawing valuable operational resources into administrative exercises while detracting from productive cybersecurity investment.
- Cybersecurity expertise being directed towards internal reporting teams and reducing the availability of skilled cybersecurity professionals for deterrence or less resourced organisations and sectors.
- Governments lacking adequate situational awareness.
- Lack of control over how sensitive information is shared.

In order to avoid multiple reporting and dispersal, there should be **single national notification entry points**. For example, incidents under CRA, NIS2 and sector specific legislation should be reported to national CSIRTs, which shall inform sectoral regulators where appropriate. These single national entry points may subsequently be connected through a single, secure, EU-wide intake portal established under CRA. The financial sector, in addition, should report based on DORA and should not be expected to widen reporting requirements to CSIRTs. This approach would improve trust and streamline the overall information-sharing framework.

It is crucial to leverage **one-stop-shop principle to report incidents**. For example, Art. 14(7) of the Cyber Resilience Act (CRA) provides a different definition of main establishment than Art. 26(2) of the NIS2 Directive. To ensure a holistic approach and improve reporting framework, entities that are in scope of both acts should use the same country of main establishment. This concept should also be integrated in other pieces of legislation. ENISA's single reporting platform developed under the CRA should be leveraged to streamline the reporting under other cybersecurity laws.

NIS2's use of '**significant incidents'** differs from the CRA's definition of '**severe incident'** or DORA's definition of **'major ICT-related incidents'**, creating inconsistencies. While they cover incidents in different domains (provision of the services versus built environment of the manufacturer), the CRA should also set geographical limits that focus on impact within the EU, as found under NIS2. Per previous statements, DORA incident reporting covers the same IT software or hardware subject to the CRA and therefore the financial sector should only report under DORA.

Additionally, all cybersecurity regulations must be aligned on what it means to '**become aware**' of the incident or vulnerability. All cybersecurity regulations should be aligned with the EDPB's guidelines on personal data breach notifications and the NIS2 Implementing Regulation 2024/269, which state that entities are considered to be aware of a breach or incident when they have a reasonable degree of certainty that a security incident has occurred.

ENISA should also consider how it can encourage further harmonisation across EU Member States regarding their **practices for submitting incident reports**. Businesses have experienced significant divergence across Member States that could contravene a business's ability to comply with EU reporting regulation. Examples include Member States with differing interpretations of how to calculate incident reporting costs, reporting submission portals refusing weekend/public holiday reports and overly cumbersome portals. All cause significant administrative burden and detract from the harmonising intentions of EU regulation.

More specifically, the EU approach to **incident reporting involves highly prescriptive data** fields and a quantitative analysis to determine whether an incident requires reporting. This often results in businesses undertaking substantial triage burden to determine if an incident reaches a specific EU criterion irrespective of its level of impact on services/products or customers. Certain classification criteria result in higher burden with limited interaction with the materiality of an incident. Recurring incidents, for instance, have high-level criteria that would result in erroneous submissions (e.g. a recurring 'change management' incident could relate to many differing facets of a change incident that have no relevance to each other). Geographic spread as a classification results in overreporting when taking account of businesses with multiple legal constructs across Member States or services/products that are provided cross-border. ENISA should further encourage means to reduce the prescriptive burden of incident reporting in the EU.

Confidentiality of the notified information should be prioritised. Therefore, the implementing act should set baseline guidance for entry points (CSIRTs):

- Notifications cannot be used as evidence against an entity.
- CSIRTs/regulators cannot disclose the fact of notification or its contents to third parties without the reporting entity's consent. Entities should own report contents, and CSIRTs/regulators must seek consent to use for any other purpose.
- Public disclosure laws should not apply to notified information.
- All information should be anonymised before potential public disclosure (which happens upon the entity's or manufacturer's consent).

Both NIS2 and CRA are missing **liability clauses** which are necessary for allowing the information to be shared in a more controlled manner. While Art 23(1) of NIS2 points that notification shall not subject the notifying entity to increased liability, the law should also clarify that they should not be liable for potential spill-over effects caused by the act of notification. Liability protections for notifying parties help promote trust and encourage information sharing in a **controlled and responsible way**, while entities should have assurances the information will not be used against them or be made public. Before a regulator can penalise for non-compliance or failure to report an incident, there should be a **cure period** after regulator notification, to comply with law by submitting a compliant incident report.

3.4. Jurisdiction

The **one-stop-shop principle** is especially helpful in cybersecurity legislation – particularly within multi-jurisdictional environments like the European Union – because it simplifies and centralises

regulatory oversight. This principle is key to the overarching harmonisation goal of NIS2, reduces regulatory burden and complexity, ensures consistency in enforcement and facilitates faster and more coordinated incident response. Unfortunately, this principle has not been adequately implemented in EU cybersecurity legislation.

The Art. 14(7) of the Cyber Resilience Act (CRA) provides a different definition of main establishment than Art. 26(2) of the NIS2 Directive. To ensure a holistic approach, entities that are in scope of both **NIS2 and CRA should use the same country of main establishment**. In addition, companies should use the same place of main establishment as a point of contact **under other legislative pieces** related to cybersecurity. Increasing the use of and consistent criteria for the main establishment principle for EU cybersecurity regulations would streamline reporting by allowing companies to submit reporting done under the GDPR, NIS2, DORA, CRA and other rules to the EU Member State of their main establishment. By way of broadening the application of the 'main establishment' principle, entities in other critical sectors should be allowed to apply the principle of main establishment if they operate in two or more EU member states.

3.5. Timelines

There are multiple challenges arising from short implementation timelines for cybersecurity legislation. While the final overall implementation deadline for performing conformity assessments under CRA is 11 December 2027, many of the most crucial requirements are not yet fully defined pending further interpretative guidance from the Commission and harmonised standards. Moreover, given varying product development cycles, in many cases the standards will not be available on time to allow manufacturers implement them before CRA enters into force. Another example is NIS2 where the ambitious transposition timeline could not be met by most member states. This resulted in fragmented implementation of NIS2 framework across the EU and challenged the key principals of NIS2 Directive, such as the main establishment.

Applying the '**stop-the-clock'** procedure would allow for proper preparation, evaluation and harmonised implementation of cybersecurity legislation. As a minimum, AmCham EU recommends extending the implementation timeline for the cybersecurity legislation, in particular CRA. In addition, the European Commission should provide guidance to EU Member States urging for phase-in periods of NIS2 requirements in general, especially considering that EU Member States are taking diverging approaches to implementing these requirements, and thus regulated entities should be given reasonable time to understand and prepare for these diverging requirements before complying with them.

3.6. Substantial modification

The concept of 'substantial modification' plays a key role in EU product law, determining when a product must undergo a new conformity assessment. Traditionally applied to physical goods, this concept becomes more complex in the context of digital products and continuous software delivery. Companies find this difficult as they continue with implementation efforts in relation to the AI Act (AIA) and the Cyber Resilience Act (CRA).

While the concept is more commonly understood within product-based sectors, the term has never been applied to the financial sector and has been introduced for the first time by the AIA and the CRA.

Intangible services, such as financial services, are separately regulated and face differing legal regimes and terminologies that are not reflected within product law. The way that "substantial modification" is defined in the law does not provide sufficient certainty that the integration of products with digital elements into business processes will not be deemed a substantial modification. This is further complicated by the potentially broad concept of "placing in the market" in the context of complex legal entity structures. Financial services will typically operate across multiple inter-affiliate legal entities where products with digital elements are provided as shared resources intragroup, without ever being provided or made available to unaffiliated customers or clients. Guidance should include confirmation that both substantial modification and placing on the market does not relate to inter-affiliate or intragroup provision of IT services.

For instance, software updates that introduce new features or alter core functionalities may raise questions about whether a re-certification is required under the CRA. The CRA attempts to address this in Recital 39, noting that modifications that alter the intended purpose or significantly increase cybersecurity risk should trigger reassessment, while routine security updates should not. However, the distinction is not always clear in practice. Ambiguity around what qualifies as a substantial modification can lead to legal uncertainty, potential over-compliance or even delays in deploying critical security patches - undermining the CRA's objectives. To address this, the Commission should issue clear and practical guidance, as mandated by the CRA, on how to assess digital modifications in line with evolving product functionality and cybersecurity risk. Such guidance should reflect the realities of agile software development and support timely, secure product updates without triggering disproportionate regulatory obligations.

4. Supply chain security

Supply chain security policy on the organisational level should be guided by considerations of a) whether a product used is secure and b) whether a product is used in a secure manner. Policymakers globally have promoted tools like Software Bills of Materials (SBOM) to be able to assess supply chain dependencies and identify vulnerabilities more efficiently. Drawing from global industry best practices, we recommend the following principles to guide the EU-level supply chain security policy.

Preserve the benefits of global supply chains. ICT products and services rely on complex, interconnected global supply chains that underpin both innovation and resilience. Overly prescriptive or sovereignty-driven requirements - such as localization mandates or ownership constraints - risk undermining interoperability, competitiveness, and technological advancement. Rather than restricting supply chains, EU policy should enable trusted, diverse, and resilient ecosystems that uphold high standards of security and transparency.

Focus on first-level relationship risk. Supply chain security policies and tools like SBOM should only focus on the first-level suppliers. Organisations should have to produce SBOMs for their suppliers, and contractually require suppliers to and provide an SBOM for their own suppliers. Frequently, it is not feasible to establish all software component across the supply chain.

Component/product identifiers. Currently, there is no single globally prescribed method for determining component names. As such, two different SBOM authors might use two different

identifiers for the same component, or the same identifier for different components. Therefore, using multiple, commonly used, hierarchical namespaces to identify software components should be allowed.

Avoid mandating a single format. Currently, three standard formats are widely used by industry: SPDX, Cyclone DX, and SWID tags. AmCham EU recommends against mandating a standard format for EU-level SBOM. Instead, industry should be allowed to determine and coalesce around best format.

Avoid SBOM for SaaS. An SBOM is only valuable when installing on-premises software and, thus, the SBOM requirements should only apply when a software product is shipped.

Avoid centralised supply chain/SBOM repositories. In order to avoid single points of failure, mandatory sharing and/or storing of SBOMs in common repositories should be avoided. SBOMs should not be made publicly available without appropriate safeguards such as nondisclosure agreements, nor be used to disclose vulnerabilities publicly, at the risk of further exposing software and their components to malicious actors.

Avoid non-technical requirements. Supply chain security policy should be guided by cybersecurity risk management principles and should not include non-technical restrictions to providers, for example based on their country of origin. Any wider security concerns should be addressed through technical controls.

Conclusion

AmCham EU is committed to constructive dialogue and partnership with EU institutions as the Cybersecurity Act evolves. The EU's goal of enhancing cybersecurity while supporting innovation, trade, and economic growth on both sides of the Atlantic is an important one. By adopting a balanced, risk-based and globally interoperable approach, the EU can set a positive example for cybersecurity policy worldwide and ensure that its digital economy remains open, secure and competitive.