ITI Promoting Innovation Worldwide

ITI's Comments on the Revision of the EU Cybersecurity Act

27 April 2026

The Information Technology Industry Council (ITI) is the premier voice, advocate, and thought leader for the global information and communication technology (ICT) industry. Our member companies include the world's leading innovation companies, with headquarters worldwide and value chains distributed around the globe. ITI's member companies represent the breadth of the technology ecosystem, including semiconductor and computer hardware and software companies, network equipment manufacturers and suppliers, cybersecurity providers, and leading Internet services and consumer technology companies. Our members are at the forefront of developing cybersecurity and privacy-enhancing technologies to ensure that citizens, institutions, and businesses are protected against cyber threats.

I. Introduction

The revision of the 2019 Cybersecurity Act is a welcome and timely initiative considering the rapidly evolving threat landscape. Financial losses caused by cybercrime continue to rise (exceeding €200 billion in avoidable losses over the past five years), underscoring the urgency of strengthening Europe's cybersecurity. Protecting critical infrastructure is essential not only for the safety, resiliency, and privacy of Europeans, but also for maintaining the competitiveness and integrity of the European Single Market. Cybersecurity is a cornerstone of Europe's technological sovereignty, and in today's threat environment it is appropriate that the EU reinforces the security and resilience of its digital supply chains.

ITI would like to provide recommendations to ensure that this revision is used to the full extent possible to improve cybersecurity and resiliency, while not undermining the economic, innovative and competitive potential of the sector and ensuring that the simplification objective is met and regulatory complexity is minimized. In particular, ITI would like to comment on the mandate of ENISA, the European Cyber Certification Framework (ECCF), the new Trusted ICT Supply Chain Framework, and the role of Simplification more broadly.

II. ENISA mandate

ITI welcomes the strengthening of ENISA's mandate and recognizes the Agency's central role in supporting Europe's cybersecurity. Acknowledging and reinforcing this role is a positive step. ITI welcomes the explicit requirement for ENISA to engage with private-sector stakeholders and the provisions in the Cybersecurity Act 2.0 proposal (CSA 2) allowing for the establishment of public-private partnerships. These measures will facilitate the co-development of guidance, certification schemes, and capacity-building initiatives. However, ITI would like to outline areas where we would like to suggest careful review of the proposed text, including the following amendments and improvements.

United States
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe
Rue Froissart 95, 1040
Brussels, Belgium
+32 (0)2 321 10 90

info@itic.org
www.itic.org
@iti_techtweets

II.1 Meaningful involvement of Industry Stakeholders:

The proposal raises concerns regarding governance and stakeholder engagement structures. The deletion of the Stakeholder Cybersecurity Certification Group (SCCG), as stipulated under Art. 22 of the current CSA, is particularly disappointing, as ITI had hoped for a modernized "SCCG 2.0" that would improve overall coordination of certification process and relevant cybersecurity experts, industry and stakeholder input. The proposed engagement mechanisms in CSA 2 are insufficient. An annual stakeholder assembly alone does not enable meaningful or sustained dialogue.

Furthermore, the mandate of ENISA's Advisory Group, as set out in Article 35(5), remains narrowly focused and these advisors are excluded from advising on topics where industry feedback could be invaluable, particularly on the application of Title III Governance for the European Cyber Certification Schemes and Title IV Security of ICT Supply Chains. To facilitate greater industry participation, we recommend that the scope of the advisory group is broadened to cover Titles III and IV and that a regular regime (such as a reformed SCCG 2.0) is set up to enable continuous and regular input regarding the development of the ECCF.

It is also important to note that, under Article 35(1), participation in the ENISA Advisory Group is limited to nationals of Member States. This may have the effect of excluding technical experts who are based in and working in the EU but hold third-country nationality. To ensure that ENISA can benefit from a broad range of expertise and perspectives, it would be beneficial to reconsider these nationality-based membership restrictions.

II.2 Security Impact Assessments (SIA):

The revision of the CSA is also a key opportunity to strengthen ENISA's role in the evolving digital policy landscape while preserving its technical and advisory functions. The CSA Revision should formalize and integrate Security Impact Assessments (SIA) as a structured process across all new tech policies and legislation, and where appropriate, the implementation of legislation and policy initiatives. This would ensure security risks are evaluated alongside economic, sustainability, and fundamental rights considerations to guarantee that the "secure-by-design" principle is also integrated across digital policymaking. We believe that "secure-by-design" is a prerequisite for Europe's resilience and defense. Just as technology itself should undergo rigorous threat modeling from the design phase onward and as this notion has been strongly integrated into the EU's cybersecurity legislation (e.g., CRA), we need to advocate a mindset in public policy that takes security into account at every step in the legislative or regulatory process.

By embedding Security Impact Assessments, ENISA can help proactively mitigate cyber risks, ensure regulatory coherence, and protect the digital single market from unintended security gaps. With its technical expertise, ENISA is well placed to turn legislative goals into secure implementation. This expanded role would also require adequate funding to support ENISA's evolving mission.

II.3 ENISA's role in the Standardization process:

We welcome and support the strengthening of ENISA's mandate, especially the participation of ENISA's technical experts in standardization development activities at Union level and at international level. However, we are concerned that the current proposal expands the Agency's role too far in ways that risk disrupting the established European and international standardization ecosystem. In particular, provisions granting ENISA authority to develop technical specifications themselves and to "lead" standardization activities could effectively position the Agency as a de facto European standardization body, operating in parallel to the European Standardization Organizations (CEN, CENELEC, and ETSI), especially in the context of certification scheme development under the European Cybersecurity Certification Framework (ECCF).

We support ENISA's strengthened role in assisting the European Commission in assessing draft harmonized standards supporting EU cybersecurity legislation and recognize the value of the Agency's technical expertise. However, industry experience consistently demonstrates that open, inclusive, and industry-led processes remain the most effective way to develop robust and widely adopted security standards. Empowering ENISA to draft technical specifications (Art. 77) or to lead standardization activities risks introducing a parallel track of technical requirements that could function as de facto common specifications, thereby bypassing the established international standardization system and undermining the essential role of international and European standardization organizations in guiding global standards development, enabling presumption of conformity through European standards, and harmonizing specifications across Member States. The current proposal does not specify who would initiate ENISA's own standards development activities, nor who would define their scope and objectives.

To preserve the integrity of the European standardization framework, the CSA 2.0 should ensure that the European Cybersecurity Certification Framework is primarily based on international and European harmonized standards. Where technical specifications are necessary, they should be defined strictly as a measure of last resort, applicable only when harmonized standards are unavailable or significantly delayed. In such cases, ENISA could develop temporary technical specifications only where a documented urgency exists, and an assessment confirms that no existing standard or specification covers the relevant scope. Any such specifications should include a mandatory withdrawal mechanism once a harmonized European standard becomes available.

In parallel, the concept of common specifications is likely to be considered in the revision of the Standardization Regulation. It is important to ensure consistency across these initiatives. CSA 2.0 should therefore be aligned with broader legislative developments, while recognizing that common specifications should be considered only as a measure of last resort.

Furthermore, the proposal should clarify ENISA's role in the standardization process by emphasizing the Agency's contribution of technical expertise rather than granting it a leading role. It should also be clarified under what circumstances, and within which Technical Committees, ENISA is expected to engage, including where it may seek leadership roles. Standardization should remain a bottom-up, industry-driven process, with leadership resting with the stakeholders responsible for implementing these standards. Redefining ENISA's role

in this way would preserve the public–private partnership model that underpins the European standardization system while ensuring that the Agency continues to provide valuable technical support to EU cybersecurity policymaking.

III. The European Cyber Certification Framework (ECCF)

The proposal takes important measures to improve the effectiveness of the EU cybersecurity certification framework. Provisions on international recognition and efforts to streamline procedures are positive developments that can enhance the global relevance and competitiveness of the certification framework.

By enabling EU cybersecurity certification schemes under certain circumstances to serve as recognized evidence of compliance with cybersecurity requirements across other applicable EU legislation, presumption of conformity will reduce the compliance burden for companies operating across multiple Member States. Important principles are also reaffirmed in the proposal: the voluntary nature of EU certification schemes; national schemes ceasing to produce effects once EU schemes are adopted; EU certification schemes focusing on technical standards only.

At the same time, several elements require careful consideration to ensure greater efficiency without compromising quality, stakeholder engagement, or Single Market coherence:

III.1 International Recognition:

We welcome the inclusion of Article 87 on the international recognition of European cybersecurity certificates. Greater international alignment is essential for globally operating companies, while recognizing that geopolitical considerations may also play a role.

Streamlining the accreditation of conformity assessment bodies (CABs) should help prevent bottlenecks and improve the efficiency of the certification system. However, Article 87 should further clarify that evaluation, auditing, and certification for EU schemes can be conducted by CABs established in third countries (and vice versa). This would be particularly relevant in the context of a potential EU-US mutual recognition agreement on cybersecurity, as referenced in the EU-US Joint Statement.

More broadly, EU certification schemes should better integrate internationally recognized standards. Where companies have already obtained globally recognized certifications, such as ISO/IEC 27001, requiring a full reassessment under EU schemes would create unnecessary duplication and additional compliance costs. The framework should therefore provide structured mechanisms for presumption of conformity or reduced assessment scope where existing certifications already cover equivalent requirements.

We are also concerned by Article 82(7), which mandates that “high” assurance assessments must take place within the EEA. Restricting the pool of eligible CABs risks creating significant

bottlenecks. Without a robust assessment of current EEA testing capacity, this requirement could delay the certification of critical high-security ICT products. Before imposing such restrictions, ENISA and the Commission should conduct a formal capacity assessment to ensure that sufficient and timely testing capabilities exist within the internal market.

III.2 Feasibility of Deadlines:

The proposed 12-month deadline for ENISA to develop a draft scheme may, on one hand, provide for effective and swift certificate scheme adoption. However, it also risks compressing timelines in a way that undermines meaningful stakeholder input and overall quality. This includes potentially neutralizing the opinions of regular international and European standardization organizations. In turn, this could affect the coherence and quality of the underlying standardization work.

Accelerating ENISA's drafting phase alone does not address the core bottleneck in scheme development, notably issues of non-technical requirements and various degrees of divergencies in cyber posture among Member States. Not all schemes can rely on existing work (like the EU Common Criteria certification scheme), which means that ENISA may have to start working from scratch on some schemes, making the 12-month deadline very unrealistic.

In preparing the request for a draft scheme, the European Commission, together with ENISA and drawing on stakeholder input, should be able to establish a timeline that reflects the specific requirements of the scheme, including extending beyond the proposed 12-month deadline where justified. This would be particularly important for schemes involving the development of new standards and would allow for adjustments where initial assessments point to greater complexity. This approach should be explicitly recognized in the body of the proposed legislation.

III.3 Stakeholder Engagement:

A clear obligation to consult stakeholders during development of the schemes is essential to ensure certification frameworks are workable and market relevant. While Article 74(2) enabling ENISA to establish ad hoc working groups is positive, ENISA and the European Cybersecurity Certification Group (ECCG) would benefit from a permanent and transparent structure providing strategic, high-level expert input into the orientation and implementation of the European Cybersecurity Certification Framework (ECCF). Industry would benefit from structured, in-person interaction with the ECCG and greater transparency on drafts and timetables for decision-making.

Industry engagement must be structured, meaningful, and embedded throughout the entire process. Industry expertise is essential to ensure that certification schemes remain practical, proportionate, and responsive to technological and market realities. As proposed above, CSA 2.0 should reinstate the SCCG, strengthened by more meaningful structural industry participation in the development and management of certification schemes. The proposed

European Cybersecurity Certification Assembly should be used for broader, high-level strategic engagement.

Furthermore, to ensure meaningful and representative input to the Assembly, Article 72 should explicitly enumerate relevant stakeholder categories, rather than relying solely on an open-ended reference to "relevant stakeholders". This could include, inter alia, ICT product and service providers (including cloud and digital service providers), SMEs, users and demand side organizations, conformity assessment and national accreditation bodies under Regulation (EC) No 765/2008, European and international standardization organizations, supervisory authorities, academia, and civil society. This clarification would improve legal certainty, balance representation, and support the Assembly's objectives.

III.4 Risks of Fragmentation Across Member States:

While Article 81(3)(c) seeks to provide flexibility in the absence of harmonized Union legislation, it risks undermining the coherence of the EU cybersecurity certification framework. Allowing Member States to attach national legal effects to European certification schemes could lead to divergent implementations built around the same certificate, weakening the Digital Single Market.

For industry, the value of EU certification lies in its predictability and uniform legal effect across Member States. National "add-ons" or differing compliance consequences would increase complexity, reduce legal certainty, and risk recreating fragmentation. It is vital that any "additions" within an extension profile remain technical in nature and are justified by specific risks or advanced security measures, as described in Recital 96. This ensures that the "single certificate" principle effectively reduces compliance costs across the Union.

If appropriately safeguarded, 81(3)(c) could help reduce duplicative audits by allowing EU certification to demonstrate compliance with national requirements. Any such approach must ensure consistent legal effects and avoid additional national requirements that would undermine harmonization.

In this context, we support the transition mechanism established in Article 86(3), which ensures that existing certificates issued under national schemes "shall remain valid until their expiry date." This "grandfathering" clause is essential to protect past investments and provide legal certainty for vendors. We therefore recommend that the date set under Article 86(1) for phasing out national schemes be made conditional on the readiness of the European certification ecosystem and be accompanied by clear and predictable timelines.

IV. ICT Supply Chain Framework

The proposal introduces a new Trusted ICT Supply Chain framework based on a multi-step, risk-based process that is, in principle, country-agnostic from the outset. ITI supports the objective of establishing an EU-wide framework to secure ICT supply chains in critical

sectors, as well as the broader goal of addressing non-technical risks associated with high-risk suppliers.

The proposal aligns with ITI's call to define a clear, objective, and risk-based framework for assessing trusted technology providers, as outlined in our recent paper, "Advancing a Vision for Effective European Tech Sovereignty." ITI's approach assesses trusted technology providers based on technical capabilities, the level of control and openness that their solutions afford to users, evaluates risk profiles with clear, consistent methodologies and, finally, by their core governance, transparency, risk management, and security practices, not their country of establishment. We appreciate the European Commission's efforts to anchor the proposed CSA 2 framework in structured risk assessments, rather than political determinations as to nationality or ownership structure, as it offers a more meaningful basis for trust and is essential to ensuring objective and evidence-based decision-making.

We welcome the proposed EU-wide approach, which has the potential to enhance harmonization, reduce fragmentation, and provide greater predictability for companies operating across Member States. The framework is particularly effective in addressing risks from state-sponsored threat actors; however, as its scope expands to a broader range of companies, it will be important to ensure that proportionality is maintained. We therefore propose targeted recommendations to clarify and refine the proposal so it can best achieve its objectives.

IV. 1 A Proportionate Approach to ICT Supplier Restrictions

The introduction of the ICT Supply Chain framework under CSA 2.0 is a constructive development, particularly in its effort to distinguish political considerations from technical certification processes. This can provide clear benefits for industry, provided that implementation is proportionate and feasible in practice. Where non-technical risks are identified as requiring non-technical mitigation, operational realities should be considered when determining the appropriate measures. This includes, for example, the availability of trusted alternative vendors and the maturity of alternative technologies. Similarly, where ICT supply chain risk mitigation measures entail restrictions or replacement obligations, sufficient transition periods should be provided, considering technical feasibility and operational continuity requirements. Where appropriate, consideration should be given to 'rip-and-replace' funding for NIS2 entities.

A structured consultation mechanism with important and essential entities, particularly those that have already gained experience from restrictions introduced under the NIS2 Directive, should be established to ensure mutual understanding of the relevant concerns and the identification of appropriate mitigation measures. Industry data is essential to assess whether a proposed phase-out timeline is technically feasible or would entail significant economic impact. At present, these considerations are not sufficiently reflected in the proposal.

IV. 2 Request for Security Risk Assessments of Third Countries (Article 99):

We understand the need for granting the Commission the ability to conduct security risk assessments directly where necessary (Article 99(3)). It is important that the conditions triggering such action are clearly defined to ensure a transparent and well-grounded process. Further specification of the criteria would be beneficial, particularly with respect to concepts such as a "significant cyber threat" and "sufficient reason to believe." The involvement of Member States, including through the NIS Cooperation Group, should remain a central element, with departure from this framework justified by robust and clearly articulated concerns. This would strike a balance between enabling timely intervention and ensuring that the instrument remains anchored in objective considerations.

We recommend amending Article 99(3) to clarify the criteria for initiating a security risk assessment and to specify the circumstances under which the Commission may bypass the NIS Cooperation Group and conduct the assessment itself. Such clarification would strengthen legal certainty, while also supporting proportionality by reserving Union-level assessments for genuinely significant and high-priority risks.

In addition, Article 99(3)(b) could benefit from the inclusion of a clear timeline for the Commission to complete its security risk assessment. This would align with the approach taken in Article 99(2), which establishes a six-month upper limit for the NIS Cooperation Group to complete Union-level coordinated risk assessments. Providing a similar deadline in paragraph 3(b) would enhance predictability and timely implementation.

Furthermore, while Article 99 provides that Union-level coordinated security risk assessments should be completed within six months, the proposal does not appear to require a comprehensive technical and economic review of the potential consequences prior to designations under Article 100. It does not foresee Impact Assessments accompanying the implementing acts adopted under Article 100(2) that designate third countries as posing cybersecurity concerns. Such safeguards may help ensure that these decisions are based on robust analysis and a clear understanding of potential implications.

IV.3 Criteria for the Designation of Third Countries as High Risk (Article 100):

The proposal places significant emphasis on designating an entire third country as a prerequisite for excluding linked entities from supply chains. This approach risks politicizing the implementation of the framework and exposing it to complex trade and diplomatic disputes. If a country-based designation mechanism is retained, the country should meet at least three of the proposed criteria for designation. A third country should only be designated where the European Commission demonstrates, based on objective criteria established into law, that its legal framework and/or pattern of behavior and practices creates a genuine conflict that renders providers unable to comply with mandatory Union law.

Article 100 includes criteria referring to situations in which third countries require entities to report vulnerabilities prior to them being known to have been exploited. The CSA 2.0 should clarify that the exploitation must be malicious, in line with the approach taken in the Cyber Resilience Act (CRA), which defines exploitation in its Article 3 definitions.

Without such qualification, security research practices, including the development of proof-of-concepts to verify and demonstrate a vulnerability, could be misinterpreted as evidence of active exploitation. As currently drafted, third countries could circumvent the CSA 2.0 criteria by requiring vulnerability reports to include a proof-of-concept, which might then be interpreted as indicating that the vulnerability has been "actively exploited."

Additionally, Article 100(1) currently permits the Commission to initiate the verification of a third country's risk profile based solely on "a public statement... of a Member State." This low threshold creates a risk that the EU-wide high-risk designation process could be instrumentalized to serve specific national political interests or bilateral tensions, rather than addressing technical cybersecurity risks relevant to the entire Single Market. We recommend raising the procedural bar to a group of at least three member states to ensure determinations are based on systemic observation rather than isolated national positions.

A similar concern arises with criterion (e) of Article 100(1), which allows the Commission to designate a country as high risk based on "relevant information stemming from… reports by Member States or international organizations." While this provision represents a key source of information for the Commission when carrying out the assessment, we recommend clarifying the organizations in scope in the article to enhance clarity regarding the nature of these reports, as well as which international organizations would be considered sufficiently competent to provide this information.

IV.4 Mitigation measures in the ICT supply chain (Article 103):

The proposal represents an important step toward strengthening the EU's capacity to address non-technical risks linked to third-country suppliers, by establishing a framework that empowers the European Commission to adopt a broad range of mitigation measures. As this framework is intended to complement existing EU legislation, it will be important to ensure continued consistency with the technical security requirements set out in NIS2, DORA, and the Cyber Resilience Act.

With regard to non-technical risks affecting critical ICT supply chains, ITI encourages that measures adopted pursuant to Articles 103(6) and 103(7) be guided by clear and objective designation criteria aligned with Article 100. This would help reinforce consistency, legal certainty, and proportionality, while ensuring that such measures are supported by appropriate justification.

Safeguarding the proper functioning of the internal market is an important Union objective and the Single Market is an important in factor in promoting business innovation and regulatory certainty across the continent. However, this objective should not be viewed in a silo from other objective assessment aspects. Thus, the reference to preserving the "internal market" as a justification for emergency measures should be carefully circumscribed. Emergency interventions should be limited to clearly identified and active cybersecurity threats, where the immediate and demonstrable security risk outweighs the potential economic and systemic consequences of market disruption.

Given that the European Single Market relies on the cross-border flow of data, services, and technologies, interventions justified primarily on internal market grounds risk creating legal uncertainty and may be subject to lengthy legal proceedings. Emergency powers should therefore be subject to clear limits, defined evidentiary thresholds, duly justified and a direct link to concrete security threats to ensure they remain exceptional and proportionate.

IV.5 Identification of High-Risk Suppliers (Article 104):

The criteria referenced for identifying high-risk vendors require more detailed definition, explanation, and safeguards. For example, the proposal indicates that the Commission may consider factors such as where a company is established, the level of control exercised by a third country, and the involvement of nationals from a third country. Our concerns regarding the use of these criteria are as follows:

- **"Where the company is established":** This could refer to the location of a company's headquarters or place of incorporation but could also be interpreted to include any jurisdiction in which the company maintains staff, subsidiaries, or operational facilities. This could be applied inconsistently and capture companies with only limited presence in a given jurisdiction. Therefore, we recommend that "establishment" be defined strictly as the jurisdiction of legal incorporation and location of ultimate effective corporate control. It is critical to avoid conflating geopolitical footprint with cybersecurity risk, or introducing other non-technical criteria here, as this should remain a security-based assessment. Moreover, the principle of what is considered a place of establishment, is already incorporated in the EU law, including the NIS2 Directive. Thus, it is highly recommended to unify any such terminology to avoid conflicting interpretations.
- **"Control by a third country":** The concept of "control" requires a clearer definition. It may refer to formal legal control based on jurisdiction and applicable rule of law, but it could also be interpreted to include broader mechanisms of hard or soft influence. Greater specificity is needed regarding the type, degree, and demonstrable nature of control required to trigger designation. The concept should be strictly limited to situations where a company is subject to undue influence by a foreign adversary or directly affiliated entity in such ways that pose a discrete security risk or could otherwise compromise the company's operational independence or the integrity of its services. It should apply only in jurisdictions where there is no appropriate, independent judicial review or meaningful right of appeal.
- **"Nationals from a third country":** Using the nationality of individuals as an indicator of supplier risk raises significant concerns. It is unclear whether the presence of a single executive or board member who is a national of a third country would suffice to designate a company as high-risk. Would a company's risk status change because of hiring a particular individual? Furthermore, under Article 104(4), would businesses

be expected to provide rosters of employees and their nationalities to enable such assessments? Using nationality as a proxy for risk would create potential discrimination concerns, and compliance burdens, without providing a reliable indicator of cybersecurity risk.

Article 104(4) establishes a presumption of high-risk status based on any form of non-cooperation. This creates a rebuttable presumption whereby a non-negligent or unwilful failure to provide requested information (potentially due to conflicting laws in the supplier's home country, the protection of trade secrets, or contractual constraints) automatically results in a "high-risk" classification. As a result, the provision effectively shifts the burden of proof onto the supplier to demonstrate that it is not controlled by a foreign government, rather than requiring the Commission to establish the existence of such control.

IV. 6 Industry Involvement:

While the definition of key ICT assets for 5G networks have been extensively consulted in the past, through national risk assessment, EU-wide risk assessment, the development of 5G toolbox, the current drafting for other sectors allows for the identification of "key ICT assets" and "threat scenarios" without mandatory consultation of industry. It is essential that industry input is an integral part of these foundational assessments, ensuring they are grounded in verifiable technical evidence, alongside the evaluation of non-technical risks conducted in cooperation with the NIS Group responsible for sectoral applications of ICT supply chain risk assessments. As these assessments effectively trigger subsequent country and vendor designations, a review mechanism should be introduced to strengthen procedural balance and allow for reconsideration where measures are not proportionate.

The European Commission should also ensure structured industry involvement throughout the risk assessment and designation process. Companies will bear the operational, financial, and legal consequences of designations and must have meaningful opportunities to provide technical expertise and market-relevant information.

IV.7 Interplay with other Union legislation

Close coordination with other European Commission initiatives will therefore be essential to avoid duplication and inconsistent obligations. For example, cybersecurity-related elements are also expected in DG ENER's forthcoming Energy Security Framework, underscoring the need to prevent overlapping requirements and ensure a coherent approach across EU policy instruments.

Further clarification would also be beneficial regarding the interaction of these provisions with other ongoing or forthcoming EU initiatives, such as the Digital Networks Act (DNA), CAIDA, the EU Space Act, and the Cyber Resilience Act. Ensuring alignment across these instruments will be important to avoid regulatory overlap and provide legal certainty for stakeholders.

V. Simplification

The proposal reiterates the European Commission's commitment to streamlining EU cybersecurity rules and reducing fragmentation across the regulatory landscape. However, the final text and the accompanying proposal for amendments to Directive 2022/2555 on measures for a high common level of cybersecurity (NIS 2 Directive) contain only limited concrete simplification measures and even introduces new obligations, which is somewhat underwhelming given earlier signals that there would be more substantial simplification within this file.

V.1 The Proposal for simplification measures and alignment with the Cybersecurity Act (NIS2 Amendments):

The NIS2 amendments introduce several targeted measures linked to the implementation of NIS2 that are intended to facilitate compliance. These include clarifications regarding scope and definitions, which may help reduce interpretative uncertainty across Member States. The proposal also excludes micro- and small-sized DNS service providers from the scope of NIS2, a welcome step toward ensuring greater proportionality.

We recommend reconsidering the inclusion of submarine data transmission infrastructure in the scope of NIS2. As noted in Recital 6 of the proposed amendments, such infrastructure is already "usually operated by entities already covered by Directive (EU) 2022/2555," including providers of public electronic communications networks, services, or cloud computing providers. Where operators are already within the scope of NIS2, they are subject to cybersecurity risk management and incident reporting obligations. Creating a separate category for submarine data transmission infrastructure would therefore add administrative complexity without meaningfully improving cybersecurity outcomes.

Importantly, the targeted NIS2 amendments aim to reduce duplicative national audits through the introduction of a new EU-level "certificate of cyber posture," which would create a presumption of conformity with NIS2 requirements. This is a significant and welcome proposal, as it has the potential to meaningfully reduce administrative burden and compliance costs for companies operating across multiple jurisdictions. The introduction of a cyber posture certification could also significantly facilitate the demonstration of compliance for companies subject to multiple EU cybersecurity regulations.

However, we strongly caution against any move to make the above mentioned "cyber posture" certification mandatory under the NIS2 regime. Transforming what should be a voluntary compliance tool into a mandatory administrative hurdle would directly contradict the Commission's goal of reducing regulatory burdens and would disproportionately impact the very entities the framework seeks to protect.

This certification framework is unlikely to be operational for at least two to three years and therefore will not provide immediate relief to companies currently navigating NIS2 implementation. The financial statement accompanying the CSA 2.0 proposal indicates that it may only be fully operational by 2033. It is therefore essential that the future cyber posture

certification be carefully aligned with existing international and Member State frameworks, rather than developed in parallel to them, in order to avoid duplication, fragmentation, or additional compliance layers.

In the interim, we support the mutual recognition of NIS2 audits across Member States as a practical and immediate step to reduce administrative burden. To this end, the proposed Article 37(a) (new) of the NIS2 Directive should be amended to ensure that, before the cyber posture certification scheme becomes fully operational, the framework for mutual assistance explicitly includes the mutual recognition of audits. This would provide an immediate and pragmatic step toward the "single audit" principle by encouraging Member States to rely on and reuse the results of audits conducted by their peers, thereby minimizing redundant compliance exercises.

At the same time, the targeted amendment introduces additional reporting obligations concerning ransomware incidents, including requirements to share potentially sensitive data. These new obligations risk creating further compliance complexity and increasing administrative burden for companies that have already adapted their internal operations to the NIS2 implementation. As currently drafted, they do not appear aligned with the broader objective of regulatory simplification and may instead introduce additional layers of reporting without clear evidence of proportional benefit. As a minimum, ransomware reporting obligations should only kick in when a ransom is paid (and not just when threats are being formulated), following the models of Australia and the United States. The risk to the ecosystem is not the prevalence of ransomware demands but rather ransomware payments, which "fuel" the ransomware ecosystem.

The NIS2 amendment also appears to expand the scope of registration information that Member States may require from entities. This includes information on where services are provided, IP ranges, and, where applicable, Business Wallet identifiers and digital addresses, as well as obligations to ensure that such information is kept up to date. While greater transparency can support effective supervision, it would be helpful to clarify whether these additional requirements will be accompanied by simplification measures. Without such safeguards, there is a risk that the expanded reporting obligations could add further complexity for entities subject to the framework.

It is also proposed that, once the Commission adopts implementing acts under Article 21(5), such as the NIS2 implementing regulation for digital service providers, Member States would no longer be able to impose any additional technical, methodological, or sector specific cybersecurity requirements on entities covered by those implementing acts. This is positive as it should in principle prevent Member States from going beyond what is mandated in the implementing regulation. Such an addition makes compliance less complicated for companies operating across the EU. This should also be expanded to Electronic Communications Services (ECS).

V.2 Further Simplification:

The European Commission had previously suggested that the revision of the Cybersecurity Act (CSA) would serve as a vehicle for more meaningful steps to reduce compliance burdens,

particularly considering the relatively modest simplification measures included in the Digital Omnibus package. In that context, expectations for more substantial relief were higher than what is ultimately reflected in the proposal. To the extent feasible, this should include the following recommendations from ITI's recent position paper on the Digital Omnibus:

- **Harmonizing definitions, reporting deadlines and requirements.** Ensure terms that are used in multiple regulations are defined consistently.
- **Reciprocity of audits.** Clarify that security and compliance audits performed under one EU regulation, beyond NIS2, qualifies towards fulfilling audit requirements under other regulations for both entities that are required to perform audits and also supervisory authorities when conducting audits. Moreover, it should be clarified that certifications and attestations such as applicable ISO certifications and SOC 2 reports may be used to fulfill audit requirements. Leveraging international best practices and fostering mutual recognition of audits will be also key to reducing duplication and complexity.
- **Reciprocity of testing.** Clarify that security testing performed under one EU regulation, such as vulnerability scans and penetration tests performed under DORA, qualifies towards fulfilling testing requirements under other EU regulations.
- **Streamlining documentation and reporting processes.** The EU should establish a single streamlined process for entities to document and report compliance with multiple overlapping regulations.
- **Harmonizing subcontractor risk management.** Regulations requiring suppliers and subcontractors to adhere to security standards should have consistent requirements, and compliance with one regulation should qualify towards compliance with others.
- **Reciprocity for standards compliance.** The EU should clarify that it provides reciprocity for compliance with internationally recognized standards and certifications such as, but not limited to, ISO 27001 and SOC2.
- **Avoid duplication in product certification requirements under CRA and NIS2.** Article 24(2) of the NIS2 Directive allows for the introduction of delegated acts requiring the mandatory use of certified ICT products. This could directly overlap with the CRA, which already establishes conformity assessment and CE marking requirements for ICT products. To avoid duplicative certification obligations and increased administrative burden for manufacturers, we recommend that CE marking under the CRA be deemed sufficient for compliance with any NIS2 delegated act on ICT product certification.