GSMA Europe and Connect Europe's views on the revised Cybersecurity Act (CSA2)

Connect Europe and GSMA Europe's views on the Revised Cybersecurity Act (CSA2)

May 2026

Connect Europe and GSMA Europe[1], representing the views of European telecommunications operators in Europe, would like to share, in the following paragraphs, their detailed reactions to the Cybersecurity Package, including the proposal for a revised Cybersecurity Act (CSA2) and amendments to the Network and Information Security Directive II (NIS2).

Connect Europe and GSMA Europe Key Remarks

The telecommunications sector is essential to economic and societal wellbeing. The sector is both a frontline defence for Europe and a clear target for malicious disruption. Telecom operators ensure strong network security and resilience through comprehensive technical, operational and organisational measures, including multi-vendor strategies included in the European Commission's 5G Cybersecurity Toolbox to mitigate risks and avoid supply chain dependencies. The measures implemented by European telecom operators are endorsed by national authorities, fulfilling national cybersecurity obligations while ensuring national competence in security matters.

Connect Europe and GSMA Europe share the European Commission's goals of reinforcing cybersecurity in Europe and largely welcome some of the changes to ENISA's mandate and the overall functioning of the European Cybersecurity Certification Framework (ECCF). However, Connect Europe and GSMA Europe are inherently concerned with the proposed ICT supply chain measures (Title IV) that go far beyond what is necessary to achieve the objectives of the regulation, and rather, risk exacerbating existing challenges faced by the telecoms sector in Europe. This includes imposing unprecedented financial, operational, and service-level burdens by mandating extensive technology removals, which overlook more proportionate assessment of risks, measures based on impacts on investment cycles, and operational implementation realities.

With the sector undergoing unprecedented technological transformation, emerging technical risks (e.g., from AI and quantum technology), will require European telecoms operators to undertake a fundamental shift in cybersecurity strategy, committing substantial financial resources and highly specialised technical expertise over the coming years. Against this backdrop, European telecoms operators must invest in modernising their networks and managing technical risks, while also meeting obligations related to non-technical risks. Striking the right balance is essential to ensure that measures addressing non-technical concerns do not inadvertently weaken capacity to respond effectively to genuine technical and innovative challenges.

In this context, the CSA2 as proposed, risks far-reaching damage to competitiveness, security and resilience, by diverting scarce resources, both in terms of investment and skilled people, away from innovation and network upgrades. The proposal prioritises a broad "rip and replace" exercise, at a time when Europe must accelerate the deployment of new networks to support 6G, AI and the quantum safe transition.

[1] DISLAIMER: The views expressed in this document are solely those of GSMA European operator members and do not necessarily represent the views, positions, or opinions of operators or other GSMA members in other regions. This document is intended to reflect the perspectives and priorities specific to the European telecommunications landscape.

Connect Europe and GSMA Europe, therefore, call for the deletion of Title IV provisions from the text, ensuring that security remains an EU Member State prerogative, respecting national frameworks, safeguarding service continuity and supporting investment. In addition, Connect Europe and GSMA Europe propose a number of adjustments to the proposal on the ECCF, the mandate of ENISA, and greater simplification.

Our key points consist of:

1. ***ICT supply chain security:*** Connect Europe and GSMA Europe call for the deletion of Title IV from the text, ensuring that national security remains a national prerogative. This allows for flexible, risk-based approaches to be taken through the prism of national realities and frameworks, while safeguarding unhindered service and investment in connectivity. The proposed Title IV, if approved, risks significantly exacerbating existing challenges faced by the sector and European industry in general. As proposed, Europe's industry and citizens would be struck with far- reaching damage to competitiveness, by diverting scarce resources away from innovation and network upgrades towards a broad "rip and replace" exercise.

2. ***The European Cybersecurity Certification Framework (ECCF):*** Connect Europe and GSMA Europe welcome the revision of the European Cybersecurity Certification Framework (ECCF). The revision presents an opportunity to significantly improve effectiveness, efficiency and transparency of cybersecurity certification processes. However, it is imperative that future cybersecurity certifications do not diverge from international cybersecurity standards to remain internationally coherent. It is also key that certifications remain purely ''voluntary'' and ensure clear and structured involvement of industry experts in their technical drafting and development to ensure they are grounded in technical and operational realities. In addition, a coherent cybersecurity posture should be ensured by avoiding multiple layers of certification; this should be based on common ground, mutual recognition of existing national certificates, the granting of equivalence where appropriate, and flexible implementation.

3. ***The mandate of ENISA:*** Connect Europe and GSMA Europe largely welcome the expansion of ENISA's mandate. However, ENISA's expanded role should preserve its independence, and focus on technical guidance, standards mapping and coordination between authorities, rather than acting as a *de facto* supervisor or policy gatekeeper.

4. ***Wider simplification/NIS2:*** Connect Europe and GSMA Europe believe that the proposed simplification efforts do not meaningfully reduce complexity and regulatory costs across EU cybersecurity law. The current proposal simply introduces additional layers of complexity rather than delivering the regulatory simplification and streamlining needed to support competitiveness and investment. Connect Europe and GSMA Europe ask for tangible simplification, enabling them to leverage its benefits while addressing legal uncertainty, avoiding additional costs and implementation complexity for industry and EU Member States. In addition, Connect Europe and GSMA Europe welcome the ambition of the Single-Entry Point (SEP) for incident reporting. However, clarity is still needed to ensure that incidents only need to be reported at national level and only once, avoiding burdensome procedures.

ICT Supply Chain Security

Key ask: Connect Europe and GSMA Europe regard the draft ICT supply chain provisions as wholly disproportionate and out of step with the intended security objectives of the CSA2 and call for the deletion of Title IV provisions of the CSA2. Rationale of the proposal follows.

Our Commitment to network security in Europe and the role of national security frameworks

The shared ambition of the European telecommunications industry is to provide a secure and trustworthy connectivity ecosystem. Building on evolving requirements, operators have developed comprehensive security concepts and implemented them in coordination with national authorities, in accordance with applicable national and EU-level requirements. These measures aim to ensure both the physical and logical protection of infrastructure and to reduce supply chain risks and dependences.

They include a holistic cybersecurity approach subject to audits and supervision complying with reporting and cooperation obligations, alongside broader strategic and organizational obligations to support the overall security and resilience of the 5G ecosystem. It includes appropriate technical, operational, and organisational measures, including the identification of critical components, regular security checks, access restrictions, network segmentation, structured processes for testing, documenting, and expediting software upgrades. Moreover, the new architectures incorporate enhanced privacy and security features compared to previous network generations. These measures effectively help mitigate potential risks.

As part of this work, operators in Europe have been diligently assessing their exposure to so-called "high-risk vendors" with the aim of addressing potential dependencies within the supply chain, adopting multi-vendor strategies beyond the provisions included in the 5G Cybersecurity Toolbox and applying them across the ecosystem. Operators have applied thorough risk-based approaches that accounts for the different threat landscapes and criticality levels of different network parts such as the Core network versus e.g., the Radio Access Network. Therefore, it is essential that the CSA2 does not introduce a one-size-fits all approach. As such, national solutions that are already implemented should not be undermined or overruled by EU intervention as they are endorsed by the competent national authorities, fit as purpose of national security and are balanced to avoid the undue impacts on national markets.

Trustworthy connectivity is a core commitment of the sector and a shared ambition with public authorities.

As an industry that plans networks on development cycles of at least ten years, policymakers must recognise the essential need for legal certainty, particularly where national measures have already been agreed and are being implemented. These frameworks reflect EU Member States' specific security circumstances and the protection of their critical national infrastructure. It is therefore vital that EU-level proposals do not contradict or override existing national decisions in ways that could disrupt ongoing implementation or impede Member States' right and responsibility to regulate matters of national security.

Financial operational and wider societal impacts of proposed ICT supply chain provisions

Should the ICT supply chain provisions remain in the text, they would create unprecedented, uncertain and highly disproportionate financial and operational impacts. Firstly, operational consequences would be severe. A multi-year rip-and-replace programme affecting all MNOs simultaneously would expose resources shortage, would degrade network performance, reduce customer experience quality and prevent the fulfilment of Europe's digital decade objectives.

Large-scale replacement, as currently envisaged, cannot be achieved without disrupting service quality and availability afforded to consumers during and after the transition. The accelerated migration of critical infrastructure increases operational instability, and quality of service.

In addition, large scale replacement would face significant operational and feasibility constraints, including limitation and workforce availability, planning capacity, field operations and customer side interventions required to execute such changes at scale.

From a financial perspective, a forced vendor replacement would significantly reduce the investment rate of all operators, small, medium and large. They would be compelled to delay, or outright halt, strategic programmes, and divert capital away from strategic growth initiatives, such as fibre expansion, 5G standalone deployment, IT modernisation and product innovation, as well as from network performance and resilience-related investments. Furthermore, the current proposal does not consider market effects and availability of necessary equipment.

Moreover, the substantial investment effort required for large scale equipment replacement would inevitably come at the expense of other priorities. As the European Commission itself highlighted in its State of the Digital Decade Report[2], at least EUR 200 billion of investment will be required by 2030 for connectivity infrastructure alone (fibre and 5G). Diverting capital towards accelerated replacement would therefore reduce resources available for these priorities, as well as for investments in cybersecurity capabilities that are essential to overall network resilience and would leave European citizens, businesses, including SMEs and public administration with fewer access and disruptive services and technologies compared to other regions.

Disproportionate framework and scope that departs from horizontal approach of NIS2

The proposed Title IV measures for the European telecoms sector are unusually broad in scope and disproportionate and should be deleted. The proposed CSA2 rather than forming a horizontal framework applicable across all sectors based on NIS2, and following a common procedure afterwards, introduces direct sector-specific measures for telecommunications that are not adequately justified.

In addition, the timeframes and scope envisaged for the prohibition or removal of equipment from suppliers, extending beyond technical risk considerations and across entire telecommunications networks, are unfeasible and do not reflect realistic deployment and investment cycles, with proposed phase-out timelines that are misaligned with infrastructure and technological lifecycles.

Moreover, compared to other identified sectors under the proposal, the telecoms sector i approach includes immediate obligations of removal, again, without appropriate justification, and thorough assessment of the impacts of such removals. The non-technical aspects of the CSA2 proposal add an unnecessary layer to an already complex regulatory and cybersecurity environment, rather than delivering the regulatory simplification and streamlining called for by the EU to support competitiveness and investment.

Lack of a robust risk-based approach and recognition of alternative risk-mitigation measures

The proposed measures are not based on sound risk and impact assessments, particularly on fixed or RAN networks. In particular, the proposal's impact assessment relies primarily on the EU coordinated risk assessment of the cybersecurity of 5G networks from 2019 and therefore cannot be used as a

[2] European Commission: State of the Digital Decade (June 2025)

basis for measures on fixed or satellite connectivity, which are not within its scope. They fail to draw on real-world lessons from previous experiences.

Risk mitigation measures should be based primarily on clearly identified, current, and tangible cybersecurity risks. Only through robust, well-established risk assessments, combined with a range of proportionate and well-defined mitigation options developed in collaboration with telecoms industry stakeholders, can co-legislators effectively determine the appropriate next steps, including whether prohibitions or phase-outs in very specific and duly justified cases would be genuinely necessary, and whether the timelines for their implementation would be feasible, taking into account the lifecycle of the current equipment and the potentially negative impacts of such extensive removals.

Additionally, there is a lack of recognition of alternative risk-mitigation measures, such as multi-vendor and diversification strategies, certification or access control to network operation, as outlined as options under the proposal. This contradicts the 5G Cybersecurity Toolbox's guidance on avoiding single-vendor dependency, which was also supported by a number of EU Member States[3], the rules of strategic autonomy and the principles of competition legislation.

The reduction to a single-vendor dependencies in network equipment markets imply the most significant risk for the European telecommunications sector, as they create single points of failure and amplify the impact of technical vulnerabilities or malicious compromise. In a rapidly evolving geopolitical context, where the classification of suppliers as "high risk" may change over time, this would effectively transform a security objective into a structural dependency and increase systemic risks to network resilience together with legal uncertainty.

In addition, from an operational cybersecurity perspective, resilience does not rely solely on the exclusion of a given supplier. It is primarily ensured through architectural diversity and multi-vendor strategies, including the coexistence of mobile, fixed and satellite networks, complementarity between operators, and vendor diversity within and across networks. These elements are central to limiting systemic risk and containing the impact of any single vulnerability, failure or attack, and should therefore be fully recognised as effective risk mitigation tools within a genuinely risk-based approach. As such, the proposed CSA2 should rather focus on technical cybersecurity risks, through the European cybersecurity framework, in line with the existing realities of the cybersecurity landscape.

Lack of certainty and level playing field: Interplay with the Digital Networks Act proposal

Additionally, regarding the reference made within the Digital Networks Act (DNA) to the CSA2 related to the obligations attached to the general authorisation and rights of use of spectrum, linking the latter to horizontal compliance regimes that have not even been adopted such as the CSA2, creates huge legal uncertainty arising from the application of different frameworks established by different competent authorities, with the resulting negative implications at all levels.. This would result in significantly stricter consequences for one sector.

Concluding remarks: proposal for deletion of Title IV – ICT Supply Chain

[3] Recent non-paper signed by FI, EE, LV, RO, IE, CZ and SI, discussed at the Competitiveness Council on 26 I'd suggest not including explicetely the question of the sanctios and insisting on : A huge regulatory uncertainty arising from the application of different frameworks established by various competent authorities, with the resulting implications at all levels. In the non-paper, those Member States support resilience through open, competitive and diverse markets, avoiding increased dependency on a limited number of suppliers.

Considering the fundamentality of security as a national concern and the risk of severe financial, operational and service disruptions of such far-reaching blanket measures, Connect Europe and GSMA Europe call for the deletion of Title IV provisions of the CSA2. The applicable framework would instead consist of the current recommendations, the Cybersecurity Toolbox and the regulation applied by National Authorities. Without making this change, Europe's industry and citizens are going to be hit with substantial disruption to the secure connectivity they rely on, with a compound effect on European competitiveness and resilience. By diverting scarce resources at a time of momentous technological change, both in terms of investment and skilled technicians, Europe risks falling further behind in its connectivity ambitions, delaying the deployment of next generation networks to support 6G, AI and the quantum safe transition.

The European Cybersecurity Certification Framework (ECCF)

Key ask: Connect Europe and GSMA Europe call for a clearer involvement of industry in developing certification schemes, balancing efficiency with effectiveness and reflecting current cybersecurity trends. Cybersecurity certifications should remain purely voluntary and not duplicate or conflict with international cybersecurity standards.

Connect Europe and GSMA Europe welcome the revision of the European Cybersecurity Certification Framework (ECCF), recognising the inefficiencies, inefficacies and transparency issues associated with the current architecture. The revision presents an opportunity to significantly improve the overall functioning of the cybersecurity certification processes.

However, it is imperative that future cybersecurity certifications do not diverge from international cybersecurity standards to remain internationally coherent. It is also key that certifications remain purely "voluntary" and ensure clear and structured involvement of industry experts in their technical drafting and development to ensure they are grounded in technical and operational realities.

The draft regulation sets a 12-month timeline for ENISA to develop certification schemes. While we see the merit in expediting certification scheme development the proposal should better balance efficiency with effectiveness. As proposed, it fails to consider the role of other stakeholders involved in their development, thereby placing disproportionate time pressures on ENISA while risking limiting the ability to produce certification schemes that are genuinely useful and implementable in practice. Recognising the timely delivery of certification schemes is key. However, ENISA should also ensure that certification schemes are compatible with industry moves towards CICD – Continuous Integration and Continuous Deployment (i.e., daily software updates put into production). We reiterate that stakeholder involvement is critical at all stages to ensure a coherent, feasible and timely implementation of legislation. A clear balance must be struck between the timeliness of certifications and their effectiveness.

A revised cybersecurity certification framework as a tool to support compliance

Connect Europe and GSMA Europe welcome the scope extension of cybersecurity certification schemes, affording entities the ability to certify their cybersecurity posture. This will support overall reinforcement of cybersecurity as well as assisting entities in Europe to meet evolving market needs.

In addition, we note that the ability to certify an entity's cybersecurity posture could support the demonstration of compliance, and allow for the presumption of conformity, with obligations stemming from the NIS2 and other relevant EU legislation. Where EU cybersecurity certifications are used as a basis for presumptions of conformity, competent authorities should, as a default, rely on the certification outcome for the requirements covered. Certification should eliminate parallel audits, duplicate evidence requests and repetitive assessments.

It should also recognise existing national certification schemes, avoiding unnecessary duplication and associated additional costs. This should be based on common ground, mutual recognition of existing national certificates, the granting of equivalence where appropriate, and flexible implementation. The simplification efficiency also depends on the cyber posture certification process, that should be reasonable to obtain and maintain. Clarity would be needed in the definition of the notion of 'cyber posture' of an entity where it refers to 'a level of cybersecurity with respect to specific security requirements' where the certification schemes are technical.

However, it is critical that the revised ECCF ensures functional cybersecurity certification schemes, based on international standards, like the ISO 27.000 series, to better support implementation of different cybersecurity-related legislation, as well as facilitating cybersecurity-by-design best practices.

In addition, given the nature of cybersecurity certification and its implementation across industry and wider society, it is crucial that the development of cybersecurity certification schemes continue to closely involve industry experts, to calibrate and build on concrete examples, requirements and best practices. We note that the Commission's proposal has effectively abolished the Stakeholder Cybersecurity Certification Group (SCCG), which remained one of industry stakeholders' few avenues for continued engagement with certification processes. While the SCCG model was imperfect, it represented a more regular forum for industry stakeholders to engage directly with ENISA and the European Commission on key issues of cybersecurity policy, particularly cybersecurity certification. Such avenues for industry engagement should not be withdrawn, but strengthened. We are concerned that the creation of the Assembly will provoke a drop in direct industry engagement. Industry expertise should be drawn upon where possible, from inception of a cybersecurity certification scheme all the way through to development and finalisation to ensure that they are fit for purpose.

The Mandate of ENISA

Key ask: Connect Europe and GSMA Europe welcome the expansion of ENISA's mandate, but caution against the Agency taking on a more operational role. We encourage the maintenance of ENISA as an independent, coordinating authority, supporting EU Member States in implementing EU cybersecurity law.

Connect Europe and GSMA Europe welcome the expansion of ENISA's mandate and resources, recognising the Agency's growing role in the European cybersecurity landscape. ENISA's expanded role should focus on technical guidance, standards mapping and coordination between authorities, rather than acting as a *de facto* supervisor or policy gatekeeper or taking on more operational duties. Preserving ENISA's independence is essential to maintain trust in certification outcomes and consistency across Member States.

ENISA's independence

The role of ENISA is regarded as valuable within the European cybersecurity landscape, particularly due to its strong technical expertise. The agency produces high-quality guidance, risk assessments, and recommendations that are widely used by Member States, EU institutions, and industry stakeholders. Its work often serves as a reference point for implementing cybersecurity requirements, contributing to a more coherent and informed approach across the Union.

CSA2 appears to transform the European Commission's role from oversight of an independent agency into an executive authority. By removing its existing mandate in the current CSA -" *When carrying out its tasks, ENISA shall act independently, while avoiding the duplication of Member State activities and taking into consideration existing Member State expertise*" (Art.3.3), and making the Commission's approval mandatory for ENISA's budget, staffing, and leadership, it effectively assumes full control of the agency's resources and governance, weakening its independence and technical credibility in the eyes of Member States and industry stakeholders. Instead of strengthening ENISA's mandate, this option undermines the agency, with no justification for altering an otherwise well-functioning independent body, even under constrained resources.

Without strong institutional independence, the technical role of ENISA would risk losing credibility. Its ability to deliver neutral and trusted expertise, support certification schemes, and guide standardisation depends directly on its independence.

ENISA's role in standardisation

The CSA2 proposal provides ENISA a role to contribute to Cyber Resilience Act (CRA) standardisation, as well as increased responsibilities to take part in European and international standards development organisations (e.g., ISO). However, we would suggest that ENISA's role in this case be limited to advising on the legal framework and providing technical guidance, rather than go down the path of drafting technical specifications.

Connect Europe and GSMA Europe believe that this will better facilitate the delivery of cybersecurity standards and more clearly developed and targeted cybersecurity certification schemes, supporting implementation of relevant EU legislation and related cybersecurity provisions. However, stakeholders should have clear and transparent means of engagement in ENISA's work on standards/cybersecurity certification.

NIS2 and broader simplification

Key ask: Connect Europe and GSMA Europe ask for tangible simplification, enabling European operators benefit from simplification while addressing legal uncertainty. This would avoid additional costs and implementation complexity for industry and Member States, and limit the increased expenses associated with the complex regulatory framework adopted over recent years.

Simplification of the current framework as a guiding principle of the CSA2

The CSA2 proposal, which was also designed and intended as a simplification instrument, should meaningfully reduce complexity and increase its utility across the ecosystem. However, the current proposal simply introduces additional layers of complexity rather than delivering the regulatory simplification and streamlining called for by the EU to support competitiveness and investment.

Secondary legislation should be limited to essential cases and encourage clear engagement with Member States and industry prior to adoption

The CSA2 proposes numerous delegated and implementing acts (19 "secondary" legislative acts) which further contribute to complexity (rather than simplification), as they offer limited opportunities for stakeholders to review and comment on specific proposals, despite the high relevance of many of these acts. By comparison, under the current CSA, implementing acts are confined to the approval of certification schemes proposed by ENISA, which we see as a more appropriate and proportionate scope for technical regulation.

Connect Europe and GSMA Europe believe that the inclusion of delegated or implementing acts should be limited to purely technical aspects, as reflected in the existing CSA, and should avoid overlaps or discrepancies with existing regulations. They should ensure a high level of engagement with all relevant stakeholders.

Real simplification of NIS2

Connect Europe and GSMA Europe are sceptical of the added value of the European Commission's proposed NIS2 simplification measures. Rather, we note that a number of the simplification initiatives add further complexity, including through additional reporting requirements.

The proposal's requirement to include deadlines for post-quantum cryptography migration in national strategies risks bringing additional obligations for entities to migrate to post-quantum cryptography (by 2030 for critical use cases and by 2035 for medium- and low-risk use cases).

We also note the reinforced provisions on ransomware. While we welcome the intentions, we are concerned that strengthened requirements for reporting ransomware-related incidents would ultimately translate into new information to be provided by the entities in notifications sent to the competent authorities or in response to requests from CSIRTs.

Finally, we also note that the provisions of Recital (9) of the proposed directive as well as Article 5(7) state that the European Commission may adopt implementing acts laying down standard formats for their supplier's forms. We believe that this risks further complexification of processes for the concerned entities, as they have already defined some forms for collecting information from their suppliers.

Connect Europe and GSMA Europe encourage co-legislators to truly address the urgent need for regulatory simplification by focusing on the ongoing overlaps between different pieces of legislation, to avoid duplicate measures, conflicting requirements and significant administrative burden for entities.

Single Entry Point (SEP) for incident reporting

A key element of ENISA's reinforced mandate, Connect Europe and GSMA Europe recognise addition of responsibilities of ENISA to develop and maintain a Single-Entry Point (SEP) for incident reporting. Legally enshrined by the proposed Digital Omnibus, albeit funded through the CSA2, the SEP could present an opportunity to simplify the reporting process for cybersecurity incidents. Connect Europe and GSMA Europe support the ambition behind the tool and see a strong need to improve on the status quo, both to reduce unnecessary bureaucracy but also to adequately support legal clarity and security incident management.

However, further clarity is still needed to ensure that incidents only need to be reported once, and it should not create further burdensome procedures instead of simplifying existing ones. In addition, Connect Europe and GSMA Europe welcome the ambition of the proposal for a SEP, which could make a significant improvement to simplify reporting requirements. The success of this tool will depend largely on how the SEP will be implemented, and the methods by which the sensitivity of the information is respected and how it will be shared.

Furthermore, currently telecom operators must report security incidents and vulnerabilities through multiple different EU and national laws, some of which have clear national contexts or national focuses. Administrative burdens should be reduced and further streamlining carried out to support reporting requirements across relevant legislation. As such, the SEP should be clearly anchored at national level for initial operational notifications, to effectively take stock of both the national and EU-level frameworks in incident reporting, considering the practical realities of incident management and cybersecurity. It should reflect the 'once-only' principle, meaning that just one notification would need to be submitted through a single-entry point in each EU Member State. The same report should then be made available to all relevant competent authorities, while fully respecting relevant requirements on IP and Trade Secrets stemming from national and EU law, as well as cybersecurity best practices in the handling and storing of such incident notification data.

Finally, the SEP should aim to avoid and remove overlapping and sectoral obligations, by ensuring that incident definitions, thresholds, reporting scopes, guidance and templates are fully harmonised and interoperable, to prevent duplication and inconsistent filings. The SEP must also ensure

confidentiality, multilingual support, legal certainty, operational reliability, secure and auditable technical mechanisms, resilient fallback channels and clear liability rules to achieve its goals, and function as a true simplification tool rather than an additional layer of compliance. In this regard, the European Commission or ENISA could provide guidance and a roadmap, to support the smooth implementation of the SEP.

Conclusion

Connect Europe and GSMA Europe recognise the ambition of strengthening ENISA's mandate and streamlining the European Cybersecurity Certification Framework. However, we maintain significant concerns with Title IV on the security of ICT supply chains based on the disruptive impacts its implementation would have. **The proposal as written has the potential to impact not only the European telecommunications sector, but the European economy and competitiveness at large including vis-à-vis its international peers**. The proposal as it stands is also at odds with the pursuit of simplification and reduction of administrative procedures recommended by the Draghi and Letta reports. Connect Europe and GSMA Europe regard the Title IV measures as wholly disproportionate, risking significant negative impacts on the European telecommunications sector. **Connect Europe and GSMA Europe therefore call on co-legislators to delete Title IV from the proposal**.

Looking ahead, a structured and continuous dialogue between the European Commission, EU Member States, the European Parliament and European telecom operators is essential to amend the CSA2 proposal, particularly to rebalance the draft law, so that it focuses on strengthening security while remaining purely risk-based, proportionate and operationally feasible. The proposal should adopt a future-proof, risk-based approach – fully respecting national security and frameworks already in force and the primary competence of EU Member States in this area.

Connect Europe and GSMA Europe invite the European Commission, the European Parliament, and EU Member States to engage constructively with industry to conduct a comprehensive risk analysis and assess the operational, financial, and customer service implications of any mitigation measures to be imposed, ensuring that the final legislation is proportionate, coherent, and operationally feasible. Doing so is vital for Europe's security and prosperity.