EUROPEAN
COMMISSION

Strasbourg, 20.1.2026
SWD(2026) 12 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT

Accompanying the documents

Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)

And

Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Executive Summary of the Impact Assessment

Objective

The primary objective of this impact assessment is to evaluate the adequacy of current regulations in addressing evolving cybersecurity threats across the EU. It proposes an integrated set of policy options aimed at strengthening the European Union Agency for Cybersecurity (ENISA), reforming the European Cybersecurity Certification Framework (ECCF) and simplifying compliance with the existing cybersecurity legislative framework. This assessment underscores the importance of modulating cyber governance to harmonize with technological advancements and market demands, while ensuring competitiveness and considering environmental impacts.

Problem Statement

Despite existing efforts, the EU's cybersecurity landscape still faces significant challenges in a context of increasingly complex threats. Insufficient coordination among Member States and other EU-level actors, stalled implementation of policy tools, and regulatory hurdles and complexity inhibit efficient cybersecurity management. These issues result in increased costs for businesses and public authorities, raised risks of cyber incidents, and inconsistent levels of protection for citizens.

Justification for EU Action

Cybersecurity threats transcend national boundaries; hence a unified approach is vital for a robust response. An EU-level intervention ensures consistent protection, enhances competitiveness by providing a level playing field, and facilitates the free movement of digital services and products within the Single Market. Harmonisation at the EU level also reduces administrative burdens through simplified compliance and streamlined procedures.

Policy Options and Preferred Option

This report analyses four areas of intervention, each with a set of policy options considered in view of the specific objectives to be achieved: (1) ENISA mandate (also part of the current CSA); (2) ECCF (also part of the current CSA) and (3) targeted amendments to the NIS2 Directive and aiming at simplification, while also interlinked with ENISA mandate and ECCF. Each of these sets of options are intervention areas on their own, while at the same time interlinked and relevant to each other.

Options to address the misalignment of the EU cybersecurity policy framework and stakeholders' needs in an increasingly hostile environment

Option A.1: *Clarifying ENISA's mandate and providing for prioritisation* - This option would ensure a clear and stable framework for the tasks of ENISA by incorporating the tasks set out by other pieces of legislation.

Option A.2: *Reforming of ENISA's mandate* - This option would repeal and replace the CSA, providing an overhaul of the Agency mandate.

Option A.3: *Reforming of ENISA's mandate with a strong operational support focus* - This option would build upon option A.2. In addition, ENISA would develop capabilities to support NIS 2 Directive entities directly in responding to and recovering from the cybersecurity incident upon Member State's request.

Options for the European Cybersecurity Certification Framework

Option B.1: *Clarifying the ECCF's scope, elements and objectives and introducing a maintenance mechanism* - This option will provide for a new maintenance mechanism of the schemes, after their adoption, to be done by ENISA.

Option B.2: *Reforming the ECCF by revising its procedures and extending the scope to facilitate simplification of regulatory compliance* - In this option, the CSA would be repealed and replaced by a new regulation. In addition to option B.1, the procedure related to request, development and adoption of schemes would be revised to improve accountability and efficiency.

Option B.3: *Reforming the ECCF as envisaged under option B.2 and introduce mandatory certification for cyberposture* - This option would build on option B.2, but aims at further strengthening the impact of the framework by introducing mandatory certification for essential entities covered by the NIS2 Directive considering specific risk scenarios, instead of relying solely on voluntary certification of entities.

Options for Simplification

Option C.1: *Taking a soft law and non-legislative instruments approach, including the use of existing empowerments (adoption of implementing acts under Article 21(5) and Article 23(11) of the NIS 2 Directive)* - This option foresees the adoption of implementing acts under the existing empowerments of the NIS2 Directive to ensure a higher degree of harmonisation of the cybersecurity risk-management measures, incident reporting thresholds, as well as information, formats and procedures of notifications, along the adoption of a set of guidelines to enhance legal certainty and harmonised implementation.

Option C.2: *Targeted intervention – further simplification of compliance with relevant Union cybersecurity legislative framework* – This option involves limited intervention through changes in the CSA and the NIS2 Directive aiming at simplifying specific aspects of the cybersecurity framework, including scope adaptations, maximum harmonisation for implementing acts, compliance proof through certification and adoption of the set of guidelines as foreseen in C1.

Option C.3: *Harmonising cybersecurity-related measures set out in Union legislation* - This option would build on option C.2 and would remove all cybersecurity risk-management measures or empowerments in relation to those included in sectorial legislation. Instead, the NIS2 Directive ecosystem would be amended to provide for streamlined requirements for all types of entities, ensuring in that way higher harmonisation.

Options for ICT Supply Chain Security

Option D.1: *Taking a soft law approach to address cybersecurity risks for ICT supply chains* - This option would not provide for regulatory intervention at EU level. Instead, the Commission would increase the number of coordinated risk assessments and voluntary toolboxes.

Option D.2: *Ad hoc regulatory intervention codifying the 5G Toolbox* - This option would codify the 5G Toolbox measures. It would introduce an obligation for Member States to ensure that components from high-risk suppliers are not used in key assets of the network.

Option D.3: *Comprehensive and horizontal framework to address ICT supply chains cybersecurity risks* - This option would establish a horizontal, technology and sector-neutral regulatory framework to address non-technical cybersecurity risks in ICT supply chains.

After extensive analyses, the preferred policy package includes: Option A.2 - Reform ENISA's mandate; Option B.2 - Reforming the ECCF by revising the procedure and extending the scope to facilitate simplification of regulatory compliance and Option C.2 - Targeted intervention – further simplification of compliance with relevant Union cybersecurity legislative framework, and Option D.3 - Comprehensive and horizontal framework to address ICT supply chains cybersecurity risks.

This combination offers a well-balanced response to identified policy challenges, significantly enhancing effectiveness, efficiency, and coherence across the EU.

Main Impacts

Cost-Benefit Analysis: The transition to the proposed regulatory framework will incur costs both for ENISA estimated up to EUR 161.3 million over five years to meet its new tasks and for public authorities across the EU of up to 80 million over five years for supervision (considering relevant cost savings). Regarding businesses, during a transition period of three years, phasing out specific high-risk equipment could lead to annual costs of EUR 3.4 to 4.3 billion for mobile network operators, while investments in trusted suppliers could grow simultaneously of up to 2 billion per year. Furthermore, streamlined and reduced compliance obligations are expected to foster cost savings for businesses of up to EUR 14.6 billion. Furthermore, significant benefits for citizens, public authorities and business would stem from improving the EU's overall cyber posture and technological sovereignty and from stimulating innovation and competitiveness, expected to largely offset initial expenditures in the long term.

Competitiveness: By reducing market fragmentation and harmonizing regulations, the preferred options enhance competitive equality across the EU, providing businesses with clearer paths to compliance and innovation.

Climate Consistency Check: The assessment considered each option's potential environmental impact. Particular attention was given to energy efficiency, travel-related emissions and infrastructure consolidation. The preferred options A.2, B.2 and C.2 have limited environmental impact, while D.3 accounts for environmental neutrality, considering

product lifecycle and transition periods for key assets replacement. This aligns with EU’s commitment to sustainability.

Digital by Default: The emphasis on streamlined digital processes demonstrates the EU's commitment to a digital-first approach, ensuring faster, more reliable data exchange and decision-making. Option D.3 could also have a high impact on digitalisation as it would entail the replacement of components from entities established in or controlled by entities from third countries posing cybersecurity concerns.

Simplification and Burden Reduction: The preferred options contribute to simplification through the introduction of scope clarifications and measures to streamline compliance and supervision, decreasing administrative burdens. The 'one-in, one-out' principle is considered by ensuring that new obligations are counterbalanced by reductions elsewhere.

Conclusion

This impact assessment presents a comprehensive strategy to enhance EU’s cybersecurity, address regulatory inefficiencies, and prepare the digital landscape for future challenges. It recommends a collaborative and cohesive approach, grounding policy reforms within existing frameworks while adapting to new technological realities. Through these measures, the EU aims to ensure a resilient, competitive, and sustainable digital economy.