EUROPEAN COMMISSION

13.11.2025

SEC(2026) 11

REGULATORY SCRUTINY BOARD OPINION

Cybersecurity Act Review

{COM(2026) 11-12}

{SWD(2026) 11-12}

EUROPEAN COMMISSION
REGULATORY SCRUTINY BOARD

Brussels,
RSB

Opinion

Title: Impact assessment / Cybersecurity Act review

Overall 2nd opinion: POSITIVE WITH RESERVATIONS

(A) Policy context

The EU Cybersecurity Act Regulation (CSA) 2019/881 established a comprehensive framework for cybersecurity in the EU. The regulation transformed ENISA into a permanent agency tasked with operational cooperation, crisis support, and managing the cybersecurity certification framework (ECCF). The ECCF was designed to harmonise and simplify cybersecurity certification across the EU, giving providers the possibility to obtain a single, recognised certificate valid across all Member States. Over time ENISA's responsibilities have expanded.

The Commission is reviewing the CSA to ensure that the ENISA's mandate, the certification system and the overall framework continue to be effective, proportionate, business-friendly, efficient for the much more complex and dynamic cybersecurity environment.

(B) Summary of findings

The Board notes improvements to the revised report responding to the Board's previous opinion.

However, the report still contains significant shortcomings. The Board gives a positive opinion with reservations because it expects the DG to rectify the following aspects:

(1) **The report does not provide sufficiently clear and robust estimates of the benefits of the intervention.**

(2) [redacted]

(3) **The report is unclear about the problems and impacts related to the simplification measures targeting the NIS2 Directive.**

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
regulatory-scrutiny-board@ec.europa.eu

(C) What to improve

(1) The report should further specify key concepts and parameters of the initiative along two axes: the distinction and interplay between technical vs non-technical cybersecurity risks, and the mandatory vs non-mandatory application of the proposed measures across the policy options.

(2) The report should provide more informative and more granular estimates of the benefits anticipated from the intervention, including avoided cyber incidents. It should further analyse the main types of incidents (malicious vs non-malicious, technical vs non-technical risks etc.), and their distribution. To the extent possible, the probabilities and costs of the diverse types of such cyber incidents need to be transparently quantified. The report should better substantiate the estimates of faster recovery times. It should better demonstrate the added value of measure on skills. An improved assessment of avoided costs and benefits for companies should be used as a basis for a strengthened analysis of effectiveness, efficiency and competitiveness.

(3) Claims regarding the effectiveness and efficiency of the intervention need to reflect any limitations and uncertainties in the analysis of benefits and costs. The assumptions and estimates underlying the main costs should be subject to sensitivity analysis. [redacted]

(4) [redacted]

(5) [redacted]

(6) [redacted] The report should clearly outline the current scope of the tasks of ENISA and the scope of ECCF and better demonstrate any identified gaps. The report should better distinguish problem drivers related to the implementation and management from those related to the scope.

(7) The report should analyse the problems, and the problem drivers related to the simplification of NIS2. The report should transparently outline possible measures including changes in the scope and assess how these measures would reduce costs for companies and what the impacts on cybersecurity would be.

(8) The report should further address the most significant gaps concerning administrative costs and cost savings, ensuring comprehensive coverage beyond businesses. Transparent classification is needed, distinguishing between compliance and administrative costs. All costs should be categorised in a

comparative manner, respecting distinctions between one-off/recurring and annual/over 5 years costs.

(9) The report should be reduced in length, avoiding repetitions, in line with better regulation requirements.

(D) Conclusion

The DG must revise the report in accordance with the Board's findings before launching the interservice consultation.

Full title	Revision of the Cybersecurity Act
Reference number	PLAN/2024/2819
Submitted to RSB on	16 October 2025
Date of RSB meeting	Written procedure

EUROPEAN COMMISSION
REGULATORY SCRUTINY BOARD

Brussels,
RSB

Opinion

Title: Impact assessment / Cybersecurity Act review

Overall opinion: NEGATIVE

(A) Policy context

The EU Cybersecurity Act Regulation (CSA) 2019/881 established a comprehensive framework for cybersecurity in the EU. The regulation transformed ENISA into a permanent agency tasked with operational cooperation, crisis support, and managing the cybersecurity certification framework (ECCF). The ECCF was designed to harmonise and simplify cybersecurity certification across the EU, giving providers the possibility to obtain a single, recognised certificate valid across all Member States. Over time ENISA's responsibilities have expanded while many stakeholders have found the certification system too complex, too slow and too costly.

The Commission is reviewing the CSA to ensure that the ENISA's mandate, the certification system and the overall framework continue to be effective, proportionate, business-friendly, efficient for the much more complex and dynamic cybersecurity environment.

(B) Key issues

The Board notes the additional information provided and commitments to make changes to the report.

However, the Board gives a negative opinion because the report contains the following serious shortcomings that the lead Service must address:

(1) **The report insufficiently defines the key concepts and scope of the initiative, and the application of its measures within the regulatory landscape.**
(2) **The report does not sufficiently explain the proposed changes to the mandate of ENISA and the reform of the EU certification framework.**
(3) [redacted]
(4) **The report does not provide robust estimates in the analysis of costs and benefits. It is also unclear about the simplification potential of the measures targeting the NIS2 Directive.**

(C) What to improve

(1) The report should clarify the key concepts and parameters of the initiative along two axes: the distinction and interplay between technical vs non-technical cybersecurity risks, both of which the report should define, and the mandatory vs non-mandatory application of the proposed measures across the policy options. While precising the scope of the revision, it should also better explain the different changes to the existing measures across relevant legislation.

(2) Given the shortcomings laid down in the evaluation of the ENISA functioning, the report should better explain their root causes, and evolving needs of the stakeholders in the changed cybersecurity landscape. It should demonstrate how the proposed expanded mandate will work, and what will warrant the success. The report should clearly describe the intervention logic regarding all main changes, including related to operational support, skills, certification and standardisation.

(3) The report should better analyse the added value of enhanced EU-level action including the changes of certification under the various options. The cost effects of introducing more far-reaching certification schemes need to be assessed.

[redacted]

[redacted]

(6) The report's assessment of the benefits, in terms of reducing the probability and impact of various cyber-incidents occurring, should be more robust. Extrapolations from a single type of incident should be avoided. The analysis of an average cost of a single type of incident should be replaced with a more granular approach taking into account various types of incidents (malicious vs. non-malicious, technical vs. non-technical risks etc.), their distribution and different costs. All key assumptions for calculations need to be presented and their robustness and related uncertainties assessed. Costs to companies for all options need to be transparently quantified and what the costs of differing types of cyber incidents might be. It also needs to be better assessed what the probability is that typical companies, of different types, might encounter specific types of incidents, (that entail different cost). An improved assessment of costs to companies should be used as a basis for a strengthened analysis of competitiveness.

(7) The report should transparently analyse the extent to which the simplification measures targeting NIS2 could reduce costs for companies, in particular the SMEs, including against the backdrop of mandatory certification would be cost-inducive, and other possible costs mentioned above. It should better assess the simplification benefits leading to a higher degree of harmonisation of the cybersecurity risk-management measures.

(8) The report should be one concise self-standing document in line with better regulation requirements, legible and accessible to the non-specialist reader.
Some more technical comments have been sent directly to the author Service.

(D) Conclusion

The DG must revise the report in accordance with the Board's findings and resubmit it for a final RSB opinion.

Full title	Revision of the Cybersecurity Act
Reference number	PLAN/2024/2819
Submitted to RSB on	27 August 2025
Date of RSB meeting	24 September 2025