EUROPEAN COMMISSION

8.7.2022

SEC(2022) 321

REGULATORY SCRUTINY BOARD OPINION

Proposal of a Regulation for the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

{COM(2022) 454}

{SWD(2022) 282, 283}

EUROPEAN COMMISSION
Regulatory Scrutiny Board

Brussels,
RSB/

Opinion

Title: Impact assessment / European cyber resilience act

Overall opinion: POSITIVE WITH RESERVATIONS

(A) Policy context

The EU cybersecurity framework comprises several pieces of horizontal legislation covering products, services, crisis management, and crimes. The European Cyber Resilience Act aims to introduce cybersecurity requirements for connected products and associated services and to complement the existing cybersecurity framework of the Directive on the security of Network and Information Systems and the Cybersecurity Act. It also complements the Delegated Regulation of 29 October 2021 under the Radio Equipment Directive, by setting up streamlined cybersecurity requirements covering a wide range of digital products and their ancillary services.

(B) Summary of findings

The Board notes the additional information provided in advance of the meeting and commitments by the DG to make changes to the report.

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 sufficiently place the initiative in the wider context of existing and proposed cybersecurity measures. It does not identify the specific regulatory gaps not already covered by the existing legislation and initiatives and the reasons why the existing measures have not fully succeeded in anticipating and addressing the problems and their drivers.

(2) The policy options do not sufficiently address all identified problem drivers and are not adequately explained in terms of content and functioning. The cost and benefit analysis is incomplete. The report does not sufficiently explain the underlying methodology and the robustness of the resulting figures attached to different options and sub-options.

(3) The report does not adequately compare options (including sub-options) in terms of effectiveness, efficiency and coherence. It does not sufficiently explain the choice, proportionality and future proof-ness of the preferred option.

This opinion concerns a draft impact assessment which may differ from the final version.

(4) The report does not systematically and transparently distinguish between the different types and views of stakeholders.

(C) What to improve

(1) The report should clearly set the scope of the initiative in the wider context of the broad range of other recent EU cybersecurity initiatives and identify exactly what specific aspect of the broader problem it aims to address. It should briefly set out, up front, all recent legislation and proposals in the area of cybersecurity and those with a cybersecurity aspect and explain the articulation between them and the initiative in terms of prevention and mitigation. It should explain in more detail the reasons why the existing body of legislation and proposals and the ongoing voluntary cyber security standards initiative have failed to address the specific issues identified in the report or to anticipate the need for further intervention. The report should better reflect the active role played by consumer awareness and behaviour in contributing to cybersecurity risks and the way in which design and default mechanisms which direct consumer behaviour may help to mitigate them.

(2) The baseline scenario should be dynamic and include all existing EU and international regulations and proposals. It should analyse what is likely to happen both in terms of the threat surface and scale given the multitude of existing tools, and acknowledge likely positive developments, either triggered by maturing legislation (or legislation currently under revision), uptake of voluntary standards or market forces. The report should provide concrete evidence of the risk of market fragmentation through national uncoordinated initiatives. The report should analyse clearly and in detail how the product liability regime affects manufacturers' ex-ante incentives to reduce consumers' exposure to cyber security risks and, in light of this assess the remaining gap to be tackled.

(3) The report should provide comprehensive options to address all identified problem drivers (including consumer behaviour) or explain why certain drivers will be not tackled while being clear how this is likely to affect the performance of the options. It should clearly explain the content and rationale and comparison of options, including sub-options. It should make sub-options more visible throughout the impact analysis right up to the comparison of options demonstrating how they impact on effectiveness or efficiency to allow for an informed choice.

(4) The impact analysis should be further developed. It should be clear about the sources for underlying figures, explain methodologies and how robust and reliable the estimates are, in particular if based on a single data source (e.g. data provided by a trade association). It should explain how the aggregate cost estimates were calculated, including for the One In, One Out approach, and ensure consistency of the figures throughout. The report should further develop the analysis of the impacts on competitiveness and innovation and the analysis of the distributional impacts for each type of stakeholders, in particular, on SMEs. Moreover, the report should further elaborate on the role and effectiveness of standardisation processes in effectively ensuring that the advocated solution is delivered in due time and sufficiently future-proof given that the digital sector is very dynamic and new technologies quickly outpace existing ones.

(5) The report should better compare options (including sub-options) in terms of effectiveness, efficiency and coherence while bringing out more clearly the related costs and benefits. In particular, the efficiency analysis should bring out more clearly the expected costs and benefits and should include the estimates of costs and benefits, the net

impact and the Benefit Cost Ratios per policy option and sub-option in the comparison table(s). On that basis, the report should further explain the choice and proportionality of the preferred option.

(6) The report should systematically and transparently reflect the views of all different stakeholders not just those whose views support the preferred option.

The Board notes the estimated costs and benefits of the preferred option(s) in this initiative, as summarised in the attached quantification tables.

Some more technical comments have been sent directly to the author DG.

(D) Conclusion

The DG may proceed with the initiative.

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

[If there are any changes in the choice or design of the preferred option in the final version of the report, the DG may need to further adjust the attached quantification tables to reflect this.]

Full title	Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for connected products and associated services (Cyber Resilience Act)
Reference number	PLAN/2022/56
Submitted to RSB on	13/05/2022
Date of RSB meeting	06/07/2022

ANNEX: Quantification tables extracted from the draft impact assessment report

The following tables contain information on the costs and benefits of the initiative on which the Board has given its opinion, as presented above.

If the draft report has been revised in line with the Board's recommendations, the content of these tables may be different from those in the final version of the impact assessment report, as published by the Commission.

I. Overview of Benefits (total for all provisions) – Preferred Option		
Description	***Amount***	***Comments***
Direct benefits		
Prevent internal market fragmentation	n/a	**Affected stakeholders:** • Hardware manufacturers and software developers
Enhanced security and transparency of digital products	n/a	**Affected stakeholders:** • Users (B2B and B2C; public authorities)
Reduced number of cyber incidents	**EUR 293.8 billion annually**	**Affected stakeholders:** • Users (B2B and B2C; public authorities) • Hardware manufacturers and software developers (as regards reputational damage)
Improvement fundamental rights and in particular protection of personal data and privacy against breaches	n/a	**Affected stakeholders:** • Data subjects (citizens and consumers)
Increased turn-over due to conformity assessment		**Affected stakeholders:** • Notified bodies
Indirect benefits		
Decrease in risk mitigation costs (such as cyber insurance etc.)	n/a	**Affected stakeholders:** • Users (B2B and B2C; public authorities)

Increased uptake of digital solutions	n/a	**Affected stakeholders:** • Users (B2B and B2C) • Hardware manufacturers and software developers • Importers, distributors • Notified bodies
Decrease in compliance costs, such as for operators of essential services under the NIS Directive and entities subject to the GDPR	n/a	**Affected stakeholders:** • Business users; public authorities
Increased global competitiveness by integrating security early in the development process	n/a	**Affected stakeholders:** • Hardware manufacturers and software developers
Positive social impact, in particular reduced number of cybercrime	n/a	**Affected stakeholders:** • Businesses • Consumers • Public authorities • Citizens
Fewer incidents with a negative environmental impact	n/a	**Affected stakeholders:** • Society as a whole
Administrative cost savings related to the 'one in, one out' approach*		
Decrease in compliance costs, such as for operators of essential services under the NIS Directive and entities subject to the GDPR	n/a	**Affected stakeholders:** • Business users
Prevent internal market fragmentation due to impending divergent national rules	n/a	**Affected stakeholders:** • Manufacturers of hardware and software

II. Overview of costs – Preferred option							
		Citizens/Consumers		**Businesses**		**Administrations**	
		One-off	**Recurrent**	**One-off**	**Recurrent**	**One-off**	**Recurrent**
	Direct adjustment costs *(triggered by security requirements, information obligations)*	N.A.	N.A.	*Familiarisation with new requirements: N.A. * Secure product development (one-off and recurrent) *Information on security of digital products: N.A.	*Secure product development: 30.5% (no BaU) - aggregated: **EUR 13.13 billion (together with life-cycle approach)** *Information on security of digital products: N.A. *Partly off-set by higher prices*	* Familiarisation with new requirements: N.A. * Appointing new market surveillance authorities (if applicable): EUR 1 600 000 per year	N.A.
	Direct administrative costs	N.A.	N.A.	*Conformity assessment: **EUR 10.6 billion**	*Creating and updating DoC, affixing CE marking and reporting: **EUR 7.8 billion**. * Accreditation framework: N.A. (notified bodies)	N.A.	N.A.
	Direct regulatory fees and charges	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.

	Direct enforcement costs	N.A.	N.A.	N.A.	N.A.	N.A.	*Monitoring and enforcement new requirements: **EUR 7.7 billion**
	Indirect costs	* Higher prices of digital products	N.A.	* Higher prices of digital products	N.A.	N.A.	N.A.
Costs related to the 'one in, one out' approach							
Total	Direct adjustment costs	N.A.	N.A.	*Familiarisation with new requirements: N.A. *Secure product development (one-off and recurrent) *Information on security of digital products: N.A.	Secure product development: EUR **13.13 billion** *Information on security of digital products: N.A.		
	Indirect adjustment costs	N.A.	N.A.	N.A.	N.A.		
	Administrative costs (for offsetting)	N.A.	N.A.	Testing: EUR **10.6 billion**	Documentation and reporting: **EUR 7.8 billion**.		