EUROPEAN COMMISSION

Brussels, 20.11.2020
SEC(2020) 430 final

REGULATORY SCRUTINY BOARD OPINION

Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

{COM(2020) 823 final}
{SWD(2020) 344 final}
{SWD(2020) 345 final}

EUROPEAN COMMISSION
Regulatory Scrutiny Board

Brussels,
RSB

Opinion

Title: Impact assessment / Revision of the Network and Information Security Directive

Overall opinion: POSITIVE WITH RESERVATIONS

(A) Policy context

The network and information security (NIS) Directive was the first internal market instrument on cybersecurity in the European Union. It aims to ensure continuity of essential services in key sectors. It focuses on threats to networks and information systems.

New challenges have emerged since the adoption of the Directive in 2016. This concerns the rapid global digital transformation, in particular. The COVID-19 crisis also demonstrates the need for efficient digital solutions.

The Directive requires the European Commission to review its functioning. This impact assessment includes an evaluation (back-to-back). The analysis investigates how to ensure cyber resilience in the internal market. It focuses in particular on entities that are vital to the economy and society.

(B) Summary of findings

The Board notes the useful additional information provided in advance of the meeting and commitments to make necessary 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 problem analysis does not sufficiently discuss how the enforcement has integrated cross-border spillovers in risk assessments of entities in key sectors.

(2) The report does not explain what success would look like for the initiative.

(3) The list of options and its justification is not exhaustive, especially regarding the sectoral coverage.

(4) The impact analysis lacks depth, in particular regarding the costs assessment.

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

Commission européenne, B-1049 Bruxelles - Belgium. Office: BERL 08/010. E-mail: regulatory-scrutiny-board@ec.europa.eu

(C) What to improve

(1) The report should reinforce the problem analysis to better focus on the problems the Directive aims to solve. It should clarify the degree of success of the initiative to date, and to which extent progress is due to international standards. The report should discuss, in particular, what cross-border problems the initiative aims to reduce and to what extent the current arrangements contribute to this objective. It should analyse whether supervisors have been able to enforce the integration of spillovers of security threats in risk assessments of key sectors.

(2) The report should explain what level of cybersecurity the revised Directive aims for. It should specify how the initiative will ensure that the right balance is struck between achieving a higher level of cyber security on the one hand and placing additional burdens on authorities and businesses on the other hand.

(3) The report should better analyse and justify the sectoral coverage. It should review the robustness of the methodology for the selection of the additional sectors for important entities, and elaborate on the weight given to different criteria and components. In particular, it should justify why the substantive sector analysis in terms of digital intensity, level of interdependency and COVID-19 importance receive only little weight when compared to stakeholders' views. This should be reflected in the explanation of the options design, including discarded options. The report should clarify the difference between the 'essential' and 'important' sectors, what criteria were used to establish those categories, and whether alternative approaches were possible. It should expand on whether the definition of sectoral coverage risks shifting the danger of exposure to other sectors. It should analyse how the choice of sectors can be made future proof.

(4) The report should include a more complete set of options on reporting, supervision and crisis response. It should include ways to interact with the linked European critical infrastructure Directive, which is also under revision. It should identify possible alternative solutions and discuss the reasons for discarding some.

(5) The report should strengthen the analysis of compliance costs, especially for medium-sized enterprises. It should provide quantitative estimates of total compliance costs under the preferred option for typical enterprises in the different sectors. It should analyse possible costs of the interaction with sectoral legislation under *lex specialis*, including from unclear provisions, multiple supervision levels or from divergences in national interpretation. The report should analyse the REFIT aspect, explaining how the initiative would endeavour to minimise regulatory burdens.

(6) The report should clarify to what extent the consultation included stakeholders from all sectors that would be added to the scope of the Directive. It should systematically present possible diverging views from stakeholder groups.

The Board notes the estimated costs and benefits of the preferred option 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	Review of the Directive (EU) 2016/1148 of 6 July 2016 concerning measures for high level of security of network and information systems across the Union ('the NIS Directive')
Reference number	PLAN/2020/7447
Submitted to RSB on	23 October 2020
Date of RSB meeting	18 November 2020

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***	***Stakeholder group main recipient of the benefits***
Direct benefits		
Reduce administrative burden by discarding the identification process		• national authorities • businesses
More clarity and further harmonisation would allow more focus on core cybersecurity tasks		• national authorities
Increase in compliance with security requirements	n/a	• businesses • national authorities
Decrease in cybercrime losses (medium/long term by implementing higher level of security requirements)	Use of higher level of security requirements and in particular fully deployed security automation (e.g. use of advanced technology, AI, automated scanning tools, etc) help companies reduce the lifecycle of a breach by 74 days compared to companies with no security automation deployment, from 308 to 234 days.	• businesses • citizens
Decrease in security incidents and cybercrime losses	Estimated reduction in cost of cyber incidents by EUR 8.6 billion over a 10-year period	• businesses • citizens
Reduction in cost liability for breaches	n/a	• businesses • citizens

Increase of trust of customers	n/a	• businesses
Protection from unfair competition (e.g. by avoiding industrial espionage)	n/a	• businesses
Increased and consistent level of resilience at the level of key businesses and cross-sector	n/a	• businesses • national authorities • citizens
Improved situational awareness	n/a	• businesses • national authorities • citizens
Increase in cybersecurity investments	An average increase of ICT security spending per sector for the next three to four years ranging from about 12% to 22% would lead to a proportionate benefit of such investments and even considerably exceed them for some sectors, notably considering that the average cost of a single data breach at the level of a sector was estimated at EUR 3.5 million in 2018, with an annual increase of about 6.4% to 13% and lost business costs account for nearly 40% of the average total cost of a data breach, i.e. about 1.30 million EUR.	• businesses • national authorities • citizens
Increased operational capabilities	n/a	• national authorities
Indirect benefits		
Improved personal data protection	n/a	• citizens

II. Overview of costs – Preferred option								
		Citizens/Consumers		Businesses		Administrations		
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent	
Action (a) ***Extension of the NIS scope (including adding a size cap)***	Direct costs	n/a	n/a	*Average 22% increase in ICT security spending for the new sectors/services added to the NIS scope in the next 3-4 years.* *For the new sectors or services, an increase of about 25% of ICT spending could be expected for medium enterprises.* *Note: overall, in addition to the estimated increase in ICT spending triggered by the extension of the sectorial scope, an average 12% increase in ICT security spending is estimated for the sectors/services currently under the scope of the NIS Directive scope in the next 3-4 years. For*	Costs of implementation of higher security requirements and documented security measures	Personnel and administrative costs leading to an overall increase of approx. 20-30% of resources of the relevant authorities per Member State at central level mainly needed for performing supervisory actions and interactions with industry (including sector-specific)	Regular personnel and enforcement costs

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

				medium enterprises, this estimate is of approx. 15%. This increase concern the cumulative effect of all measures envisaged by the preferred option.			
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
Action (b) ***Discarding the identification process and putting all operators and digital service providers under an equal footing, while differentiating on importance/criticality grounds***	Direct costs	n/a	n/a	Negligible personnel costs (notably legal departments), no additional FTE	n/a	n/a	n/a
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
Action (c) ***Further harmonising and streamlining risk management/security requirements***	Direct costs	n/a	n/a	• Personnel (including potentially setting up new in-house teams): 2 -4 extra FTEs • Administrative costs • Opportunity costs • Potential increase in purchase costs on cybersecurity of +10-15%.	• Purchase costs (consultancy, audit, penetration tests, etc.)	Approx. 20-30% increase in budget/expenses), same increase as triggered by supervisory and enforcement-related measures + administrative costs for the sector-specific decentralised models for the new sectors/services to be added to the NIS scope	Recurrent personnel and technical costs (audits, testing, etc).

	Indirect costs	Potential slight increase in prices of products as a result of investment in cybersecurity technologies and measures	n/a	n/a	n/a	n/a	n/a
Action (d) ***Security elements concerning supplier relationships and supplier-specific risk assessment***	Direct costs	n/a	n/a	• Personnel - in average 1 FTE • Purchase costs (consultancy, audit) • Opportunity costs	• Personnel and potential regular outsourcing for risk assessments (notably for SMEs):potential increase of 2-4% in recurrent purchase ICT security costs	• Part of the overall 20-30% increase in budget/expenses) trigged by the extended NIS scope, further harmonisation of security requirements and enhanced supervisory activities. • 1-2 FTEs (legal and technical background)	Regular personnel costs
	Indirect costs	Potential slight increase in prices of products as a result of investment in cybersecurity technologies and measures	n/a	n/a	n/a	n/a	n/a
Action (e) ***Streamlining incident***	Direct costs	n/a	n/a	Personnel costs – potentially 1-2 FTE/organisation	Regular personnel costs	Personnel costs (1-2 FTEs)and potential purchase of software (including for reporting	Regular personnel costs)

notifications						summary of incident reports to ENISA)	
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
Action (f) ***Reinforcing and further harmonising supervision and enforcement***	Direct costs			Personnel (2FTE/organisation) and purchase costs (in particular for DSPs and SMEs)	Regular personnel costs and potential increase in outsourcing, notably for audits (in particular for SMEs and DSPs) – overall additional 5% of recurrent purchase costs	Part of the overall 20-30% increase in budget/expenses) + administrative costs for the sector-specific decentralised models for the new sectors/services to be added to the NIS scope + 1-2 additional FTEs per competent authority	Personnel Purchase costs Administrative costs
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
Action (g) ***Incentivising the increase in Member States resources for and prioritising of cybersecurity policies (e.g. peer review and mutual assistance***	Direct costs	n/a	n/a	n/a	n/a	• For the mutual assistance mechanism: 2-3 FTEs per CSIRT team) • For the peer-review:	Personnel and costs triggered by operational activities – in average 5,000 EUR per year per authority for peer-review missions – partially supported by the EU's Digital Europe Programme

mechanism)	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
Action (h) ***Strengthening cooperation and information sharing (including through ISACs with public authorities participation)***	Direct costs			Personnel costs – 1 extra FTE/organisation	More involvement in the public-private partnerships and ISACs – recurrent personnel costs (*medium level*)	Personnel costs – 1-2 FTEs	Regular personnel costs
	Indirect costs						
Action (i) ***Incentivising coordinated vulnerability disclosure***	Direct costs			Negligible personnel costs (could, use existing FTEs who would monitor an additional input channel)	Negligible personnel costs	• Part of the overall 20-30% increase in budget/expenses) trigged by the extended NIS scope, further harmonisation of security requirements and enhanced supervisory activities. • Personnel (1/2 FTEs) • Administrative costs • In-house R&D	Regular personnel and purchase/maintenance costs
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
Action (j) ***Setting up a crisis management framework***	Direct costs	n/a	n/a	n/a	n/a	Personnel: 3-4 FTEs/national authority and administrative costs	• Personnel • Administrative costs (participation in

focused on operational cooperation							exercises, operational exchange)
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a

(1) Estimates to be provided with respect to the baseline; (2) costs are provided for each identifiable action/obligation of the preferred option otherwise for all retained options when no preferred option is specified; (3) If relevant and available, please present information on costs according to the standard typology of costs (compliance costs, regulatory charges, hassle costs, administrative costs, enforcement costs, indirect costs; see section 6 of the attached guidance).