EUROPEAN
COMMISSION

Brussels, 16.12.2020
SWD(2020) 344 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT

Accompanying the document

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} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Executive Summary Sheet

Impact assessment on the *Review of Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereinafter 'the NIS Directive')*

A. Need for action

What is the problem and why is it a problem at EU level?

In spite of its notable achievements, the NIS Directive, which paved the way for a significant change in mind-set, institutional and regulatory approach to cybersecurity in many Member States, has by now also proven its limitations. The digital transformation of society (intensified by the COVID-19 crisis) has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses. The number of cyber-attacks continues to rise, with increasingly sophisticated attacks coming from a wide range of sources inside and outside the EU.

Based on the evaluation on the functioning of the NIS Directive, the Impact Assessment identified the following problems: the low level of cyber resilience of businesses operating in the EU; the inconsistent resilience across Member States and sectors and the low level of joint situational awareness and lack of joint crisis response. For example, as a result of some of these problems and drivers, there are situations where major hospitals in a Member State do not fall within the scope of the NIS Directive and hence are not required to implement the resulting security measures, while in another Member State almost every single hospital in the country is covered by the NIS security requirements.

What should be achieved?

Three general objectives are envisaged with the NIS review:

1. **Increase the level of cyber resilience of a comprehensive set of businesses operating in the European Union across all relevant sectors,** by putting in place rules that ensure that all public and private entities across the internal market, which fulfil important functions for the economy and society as a whole, are required to take adequate cybersecurity measures.
2. **Reduce inconsistencies in the resilience across the internal market in the sectors already covered by the Directive,** by further aligning (1) the de-facto scope, (2) the security and incident reporting requirements, (3) the provisions governing national supervision and enforcement and (4) the capabilities of competent authorities in the Member States.
3. **Improve the level of joint situational awareness and the collective capability to prepare and respond,** by taking measures to increase the level of trust between competent authorities, sharing more information and setting rules and procedures in the event of a large-scale incident or crisis.

What is the value added of action at the EU level (subsidiarity)?

Cybersecurity resilience across the Union cannot be effective if approached in a disparate manner through national or regional silos. The NIS Directive came to address this shortcoming, by setting a framework for network and information systems security at national and Union levels. However, its transposition and implementation also brought to light inherent flaws of certain provisions or approaches, such as the unclear delimitation of the scope of the NIS Directive. Furthermore, since the COVID-19 crisis, the European economy has grown more dependent on network and information systems than ever before and sectors and services are increasingly interconnected. The first periodical review of the NIS Directive created therefore the opportunity for further EU action. The EU intervention going beyond the current

measures of the NIS Directive is justified mainly by: (i) the cross-border nature of the problem; (ii) the potential of EU action to improve and facilitate effective national policies; (iii) the contribution of concerted and collaborative NIS policy actions to effective protection of data protection and privacy.

B. Solutions

What are the various options to achieve the objectives? Is there a preferred option or not? If not, why?

The Impact Assessment analysed four policy options: (0) maintaining the status quo; (1) non-legislative measures to align the transposition; (2) limited changes to the NIS Directive for further harmonisation; (3) systemic and structural changes to the NIS Directive. Option 1 was discarded at an early stage as it does not depart considerably from the status quo. The Impact Assessment concludes that the **preferred option** is option 3 (i.e. **systemic and structural changes to the NIS framework**), as it would envisage a more fundamental shift of approach towards covering a wider segment of the economies across the Union, yet with a more focused supervision targeting proportionally big and key companies, while clearly determining the scope of application. It would also streamline and further harmonise the security-related obligations for companies, create a more effective setting for operational aspects, as well as establish a clear basis for shared responsibilities and accountability of relevant actors and incentivise information sharing.

What are different stakeholders' views? Who supports which option?

The majority of competent authorities and businesses showed support for a revision of the NIS Directive. Throughout several consultations, they signalled that a reviewed NIS Directive should cover additional (sub)sectors, align or streamline further security measures and reporting obligations. Stakeholders also showed support for new concepts or policy-related measures that are only part of the preferred option (e.g. supply chain security policies, institutionalisation of an operational EU crisis management framework).

C. Impacts of the preferred option

What are the benefits of the preferred option (if any, otherwise of main ones)?

The preferred option would bring significant benefits: estimates made based on an economic modelling developed by a support study for the NIS review indicates that the preferred option may lead to a reduction in cost of cybersecurity incidents by EUR 11.3 billion.

The sectoral scope would be considerably enlarged under the NIS framework, but next to the above benefits, the burden that may be created by the NIS requirements, notably from the supervision perspective, would also be balanced for both the new entities to be covered and the competent authorities. This is because the new NIS framework would establish a two layer approach, with a focus on big and key entities and a differentiation of supervisory regime that allows only ex post supervision (i.e. reactive and without a general obligation to systematically document compliance) for a large number thereof, notably those considered ‘important’ yet not ‘essential’.

Overall, the preferred policy option would lead to efficient trade-offs and synergies, with the best potential out of all policy options analysed to ensure an increased and consistent level of cyber resilience of key entities across the Union that would eventually lead to cost savings for both businesses and society.

What are the costs of the preferred option (if any, otherwise of main ones)?

The preferred policy option would lead to certain compliance and enforcement costs for the relevant

Member States authorities (an overall increase of about 20-30% of resources was estimated). However, the new framework would also bring substantial benefits through a better overview of and interaction with key businesses, enhanced cross-border operational cooperation, as well as mutual assistance and peer-review mechanisms. This would lead to an overall increase in cybersecurity capabilities across Member States.

For the companies that would fall under the scope of the NIS framework, it is estimated that they would need an increase of maximum 22% of their current ICT security spending for the first years following the introduction of the new NIS framework (this would be 12% for companies already under the scope of the current NIS Directive). However, this average increase of ICT security spending would lead to a proportionate benefit of such investments, notably due to a considerable reduction in cost of cybersecurity incidents (estimated to EUR 11.3 billion over ten years).

What are the impacts on SMEs and competitiveness?

Small- and micro-businesses would be exempted from the scope of the NIS framework under the preferred option. For medium-sized enterprises, it can be expected that there would be an increase in the level of ICT security spending in the first years following the introduction of the new NIS framework. At the same time, raising the level of security requirements for these entities would also incentivise their cybersecurity capabilities and help improve their ICT risk management.

Will there be significant impacts on national budgets and administrations?

There would be an impact on national budgets and administrations: an estimated increase of approximately 20-30% of resources would be expected in the short and medium term.

Will there be other significant impacts?

No other significant negative impacts are expected. The preferred policy option is expected to lead to more robust cybersecurity capabilities and consequently would have a more substantial mitigating impact on the number and severity of incidents, including data breaches. It is also likely to have a positive impact on ensuring a level playing field across Member States of all entities covered under the NIS scope and reduce cybersecurity information asymmetries.

Proportionality?

The preferred option does not go beyond what is necessary to meet the specific objectives satisfactorily. The envisaged alignment and streamlining of security measures and reporting obligations relate to the Member States and businesses' requests to improve the current framework.

D. Follow up

When will the policy be reviewed?

The first review would take place 54 months after the entry into force of the legal instrument. The Commission would provide a report to the European Parliament and the Council on its review. The review would be prepared with support of ENISA and the Cooperation Group.