European Commission

COMBINED EVALUATION ROADMAP/INCEPTION IMPACT ASSESSMENT

This combined evaluation roadmap/Inception Impact Assessment aims to inform citizens and stakeholders about the Commission's work in order to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities. Citizens and stakeholders are, in particular, invited to provide views on the Commission's understanding of the current situation, problem and possible solutions and to make available any relevant information that they may have, including on possible impacts of the different options.

TITLE OF THE INITIATIVE	*Revision of the NIS Directive*
LEAD DG – RESPONSIBLE UNIT – AP NUMBER	*CNECT/H2*
LIKELY TYPE OF INITIATIVE	*Legislative proposal*
INDICATIVE PLANNING	*Q4 2020*
ADDITIONAL INFORMATION	*https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive*

This combined roadmap/Inception Impact Assessment is provided for information purposes only. It does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content. All elements of the initiative described by this document, including its timing, are subject to change.

A. Context, Evaluation, Problem definition and Subsidiarity Check

Context

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive) is the first horizontal internal market instrument aimed at improving the resilience of networks and systems in the Union against cybersecurity risks. It has introduced concrete measures building cybersecurity capabilities and mitigating growing threats to network and information systems used to provide essential services in seven vital sectors for the EU economy and society, which rely heavily on ICT (energy, transport, banking, financial market infrastructures, health, water supply and distribution and digital infrastructure), as well as for key digital service providers (online marketplaces, online search engines and cloud computing services). The Directive obliges these undertakings to report major security incidents to the competent national authorities.

As part of its key policy objective to make “Europe fit for the digital age”, the Commission announced in its Work Programme 2020 that it would review the NIS Directive by the end of 2020. This would advance the deadline foreseen under Article 23(2) of the Directive, according to which, the Commission shall review the functioning of the Directive and report to the European Parliament and the Council by 9 May 2021. This is further justified by the sudden increase in the dependence on information technology during the COVID 19 crisis.

Depending on the results from the evaluation of the functioning of the NIS Directive, an open public consultation and an impact assessment, the Commission might propose measures aimed at enhancing the level of cybersecurity within the Union.

In order to ensure consistency and coherence with related Union legislation, the NIS Directive review will in particular take into account the following Commission initiatives:

- the review of the European Programme for Critical Infrastructure Protection (also planned for Q4 2020),
- the initiative on a digital operational resilience act in the financial sector (DORA) (planned for Q3 2020),
- the initiative on a network code on cybersecurity with sector-specific rules for cross-border electricity flows.

Evaluation

The review will evaluate the functioning of the NIS Directive based on the level of security of network and information systems in the Member States.

In accordance with the Better Regulation Guidelines, the evaluation will assess the effectiveness, efficiency, coherence, relevance and EU added value of the NIS Directive taking into account the constantly evolving technological and threat landscape. It will pay attention to the impact of the NIS Directive on increasing the levels of cybersecurity across the Union, in particular on the level of national cybersecurity capabilities and the capacity to mitigate growing security threats to network and information systems used to provide essential services in key

sectors. The evaluation will elaborate on the lessons learned from the implementation of the NIS Directive and identify persisting and emerging issues affecting the functioning of the Directive.

The evaluation will also identify and quantify the direct and indirect regulatory costs and benefits resulting from the implementation of the NIS Directive. The evaluation will focus on the period starting from the end of the transposition deadline in May 2018 and cover all Member States.

Problem the initiative aims to tackle

As provided by Article 23(1) of the NIS Directive, the Commission has already started the process of reviewing the functioning of the NIS Directive with a report that assessed the consistency of Member States' approaches in the identification of operators of essential services (OES Report). In addition, in view of its obligation under Article 23(2) to report on the functioning of the Directive, the Commission has been carrying out "NIS country visits" across the Member States since June 2019. Moreover, the implementation of the NIS Directive has been the subject of the discussions with the Member States' competent authorities in the NIS Cooperation Group and its work streams.

Based on the evidence gathered up to date, the Commission observed that the NIS Directive has largely contributed to improving the cybersecurity capabilities within the Member States and the level of protection of network and information systems throughout the Union. However, a number of issues related to the implementation of the Directive became apparent.

Member States have opted for very different approaches when implementing the Directive because of the minimum level of harmonisation and the identification process applicable to operators of essential services, which leaves a wide margin of discretion to the Member States. This has led to significant inconsistencies and fragmentation in the regulatory landscape, which may undermine the level playing field for some operators and lead to further fragmentation of the single market. As a result, some sectors and actors with critical societal and economic activities, which are as vulnerable to cyber incidents and risks as the operators covered by the Directive, are left outside its scope. Operators providing essential services in different Member States have to comply with diverging security and incident reporting regulatory regimes, which creates an additional burden for those entities. With regard to the digital service providers and in view of the constantly growing importance of their services for the society and economy, an assessment of the regulatory approach applied to them appears to be necessary.

In addition, the speedy digital transformation of our society has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses. The COVID 19 crisis and the resulting sudden growth in demand for internet-based solutions has emphasised even more the need for a state of the art cybersecurity. To this end, further enhanced and structured information sharing between stakeholders will be prerequisite for the effective countering of cyber threats.

Basis for EU intervention (legal basis and subsidiarity check)

The legal basis for the NIS Directive is Article 114 of the Treaty on the Functioning of the European Union, whose objective is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules.

In the present case, Union intervention in the area of cybersecurity is justified on grounds of subsidiarity due to the cross-border nature of the risks and the negative impact that a fragmented and purely Member-State-driven approach to cybersecurity would have on the internal market. Joint action at Union level would therefore result in more effective protection against cyber threats (and thus add value to existing national policies).

Any proposed actions would build on the objectives of the current NIS Directive of ensuring an adequate level of protection against cybersecurity threats across the Union. Furthermore, they would improve the level playing field for companies in the internal market. Any new legislative act would therefore have the same legal basis as the current NIS Directive.

B. Objectives and Policy options

In order to achieve a "Europe fit for the digital age", the Union has to ensure a state of the art response reflecting the new needs for increased cybersecurity. Such a response should aim in particular at increasing preparedness at national and Union level by building up robust Member States' and Union's capabilities to prevent, detect, respond to and mitigate cyber threats and be prepared to act in crisis. Furthermore, it should enhance cyber resilience of all key economic sectors and reduce fragmentation of the internal market by increasing the level of harmonisation of requirements applied to entities in those sectors. It should as well be coherent with other

relevant sectorial legislation.

At this preliminary stage of reflection, the Commission is considering the following possible policy options to address these objectives:

1) The baseline scenario used as a benchmark for the assessment of the policy options is the current situation including the expected evolution in the implementation of the NIS Directive.
2) Non-legislative measures could be considered as a stand-alone policy option aiming to support certain elements of the current Directive. In particular, guidelines could address less harmonised areas of the Directive such as the identification of operators of essential services with the purpose of avoiding significant inconsistencies in the application of provisions leading to fragmentation in the regulatory landscape.
3) A second option of regulatory intervention could consist in introducing targeted changes to the current NIS Directive with a view to clarifying certain provisions and improving harmonisation of the current rules. In particular, the Commission could propose to amend some definitions used for the purposes of the Directive, introduce more harmonised elements in the process of identification of operators of essential services, as well as expand the scope of the Directive with the aim to cover other sectors or services, which are equally essential for the functioning of the society and economy as the operators of essential services and the digital service providers in the scope of the current Directive.
4) Another policy option could be a legislative act that would repeal the NIS Directive, and that would aim to achieve a higher level of harmonisation and consistency by means of more detailed and precise rules. It would streamline to a large extent processes and requirements introduced by the NIS Directive framework and thus reduce significantly the fragmentation of the internal market. Furthermore, it would extend the scope of the Directive to other sectors or services not currently covered by the Directive while introducing new policy measures such as in the area of information sharing in order to meet better the needs for increased cybersecurity.

The Impact Assessment will investigate the various policy options, including non-legislative measures and possible regulatory interventions, as well as a combination of the two.

C. Preliminary Assessment of Expected Impacts

Likely economic impacts

Addressing the currently persisting insufficiency of cybersecurity preparedness at a Member State level and at the level of companies and other organisations could result in efficiency gains and reduction of additional costs resulting from cybersecurity incidents.

- For operators of essential services and digital service providers, and especially in the case of SMEs, increasing the level of cybersecurity preparedness could result in mitigating potential loss of revenue due to disruptions – including from industrial espionage - and could reduce the large expenses for an ad-hoc threat mitigation. Such gains are likely to outweigh the necessary investment costs. Achieving a level playing field for operators could also allow for fairer competition among operators.
- For Member States, it could further reduce the risk of growing budgetary expenses for ad-hoc threat mitigation and additional costs in case of emergencies related to cybersecurity incidents.
- For citizens, addressing cybersecurity incidents it is expected to result in reduced loss of income due to economic disruption.

The increased levels of cybersecurity across the Member States and the ability of companies and authorities to respond quickly to an incident and mitigate its impact will most likely result in an increase of the overall trust of citizens in the digital economy, which might have a positive impact on growth and investment.

Likely social impacts

Increasing the overall level of cybersecurity is likely to lead to an increased overall security and smooth uninterrupted functioning of essential services, which are critical for the society. The initiative may also contribute to other social impacts such as reduced levels of cybercrime and terrorism and increased civil protection. Increasing the level of cyber preparedness for businesses and other organisations may avoid potential financial losses as a result of cyberattacks thus preventing the need to lay off employees.

Likely environmental impacts

Increasing the overall level of cybersecurity could lead to the prevention of environmental risks/damage in case of an attack on an essential service. This could be particularly valid for the energy, water supply and distribution or

transport sectors. By strengthening the cybersecurity capabilities, the initiative could lead to more use being made of latest generation ICT infrastructures and services that are also environmentally more sustainable and to the replacement of inefficient and less secure legacy infrastructures. This is expected to contribute also to reducing the number of costly cyber incidents, freeing up resources available for sustainable investments.

Likely impacts on fundamental rights

Increasing the level of cybersecurity and creating a level playing field for all operators falling in the scope of the NIS Directive would most likely lead to improved personal data protection as a result of a reduced number and severity of incidents including data breaches.

Likely impacts on simplification and/or administrative burden

Simplification and burden reduction potential on relevant entities will be looked at it in each policy option. Increasing the level of harmonisation, including by streamlining security and incident reporting requirements is expected to result in a reduction of regulatory costs (the administrative burden and of compliance costs) for entities that have to apply requirements stemming from divergent national laws implementing the Directive. Streamlining incident-reporting requirements could also remove the burden of having to notify the same incident to different national authorities.

D. Evidence base, Data collection and Better Regulation Instruments

Impact assessment

An Impact Assessment, including impacts on fundamental rights and in particular on the right of personal data protection will help preparing the policy initiative, supported by an evidence collection exercise and a stakeholder consultation process and the evaluation. It will be prepared in full alignment with the Better Regulation Guidelines. The Impact Assessment will also benefit from substantial consultation actions that have been taking place since 2019.

Evidence base and data collection

To date, the Commission has been carrying out conformity checks with a view to assessing the compatibility of the national implementing measures with the Directive's provisions. Since June 2019, the Commission has been organising country visits to gather feedback on the implementation and functioning of the Directive from numerous stakeholders. So far, the Commission has collected information from over a hundred stakeholders, including essential services operators, digital service providers and the national competent authorities.

Moreover, under Article 23 (1) of the NIS Directive, based on the information provided by the Member States, the Commission adopted in October 2019 a report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services (OES Report).

The Commission has been collecting feedback on the functioning of the Directive from all participating Member States' authorities and the European Union Agency for Cybersecurity (ENISA) also in the framework of the NIS Cooperation Group.

The results from the country visits, the conclusions from the OES Report and feedback from the NIS Cooperation Group discussions will feed into the evaluation of the functioning of the current NIS Directive according to Article 23(2) as well as into the impact assessment.

In addition to its past and ongoing actions, the Commission will collect evidence via a public consultation, desk research, expert interviews, workshops with experts and focus groups with representatives of national authorities of Member States and businesses in the relevant sectors under scrutiny, as well as other stakeholders. The Commission will be supported by an external study, which will provide input to the evaluation and drafting of the impact assessment.

Consultation strategy

The consultation activities aim at collecting the views of Member States' competent authorities, Union bodies dealing with cybersecurity, operators of essential services, digital services providers, companies in other vulnerable sectors outside the scope of the current NIS Directive, trade associations, researchers and academia, cybersecurity industry professionals, consumer organisations and citizens.

It will include an open public consultation to be carried out for a 12-week period. The expected starting date of the consultation will be in July 2020. It will include questions regarding all elements of the NIS Directive in order to gather information for the retrospective evaluation. It will also focus on policy options for a potential revision of the Directive. The aim is to collect diverse opinions and experiences from all stakeholder groups. Expert interviews, workshops with experts and focus groups with representatives of national authorities of Member States and businesses in the relevant sectors under scrutiny and targeted surveys will be organised to gain a deeper

understanding of current cybersecurity challenges, the evolving threat landscape and to discuss policy options for a potential revision of the NIS Directive.

Three regional workshops (likely in a virtual format) will be organised gathering Member States, representatives of competent authorities, operators and cybersecurity experts. They will take place in the third quarter of 2020.

Will an Implementation plan be established?

If a directive were to be proposed, an implementation plan will be established. In the case of a regulation, an implementation plan is not envisaged.