Ref. Ares(2012)1257774 - 24/10/2012

EUROPEAN COMMISSION
Impact Assessment Board

Brussels,
D(2012)

Opinion

Title **DG CONNECT - Proposal for a Directive of the European Parliament and of the Council to ensure a high level of network and information security across the Union (draft version of 18 October 2012)***

(A) Context

This impact assessment focuses on Network and Information Security (NIS) across the EU. It aims at identifying appropriate measures to improve the level of preparedness and enhance cooperation, coordination and information exchange in the area of NIS amongst the Member States and between market operators and the Member States. Under Article 4(c) of Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency (ENISA): "network and information security" means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

(B) Overall assessment

While the report has been improved in line with most of the recommendations in the Board's first opinion, the justification for imposing some of the measures proposed, such as reporting, risk management and mandatory cooperation requirements, on a very wide range of public bodies and industrial sectors, including SMEs, is still lacking. Given the range of measures already in place, the report should better explain the added value of these proposals, presenting and explaining where the gaps in the current measures are. Second, given that the report has now identified the sectors to be covered, it should justify the proportionality of imposing measures, including costs, across these specific sectors including SMEs, the health sector and local authorities. Third, it should explain why cooperation between Member States is best achieved by regulatory intervention. Fourth, it should still provide more detail on the content of the preferred option in particular, and show how this will work in practice. Fifth, the report should still strengthen its assessment of significant impacts including **social/employment impacts, competitiveness, data protection and international aspects. Finally, the report should provide more analysis on the results of the public consultation and include an operational plan for future evaluation.**

* Note that this opinion concerns a draft impact assessment report which may differ from the one adopted

(C) Main recommendations for improvements

(1) Strengthen the problem definition. While the report better describes the range of existing requirements already in place (such as data protection obligations, critical infrastructure etc.) it should still highlight where exactly are the gaps that not already covered by these measures. To strengthen this aspect the report should include a table showing the extent to which issues are already addressed by existing obligations and what needs to be covered by new proposals. Given the range of measures that are already in place, the report should also better clarify how duplication of requirements would be avoided. The report should also better explain why there is an apparent lack of trust and why companies or public sector organisations are not motivated to ensure adequate investment in security and risk management. Given that the report has now clarified the sectors to be covered by the proposals, it should provide a deeper analysis of the nature of the risks in these specific sectors including the extent to which, and how, networks and/or services may be affected. In general the report should strengthen the evidence base, beyond relying mainly on the responses to the public consultation, to demonstrate why these sectors (such as health, SMEs and local authorities) have been included and why others (e.g. micros) can be considered not relevant. The report should better include the different views of stakeholders', in particular of Member States' authorities and private companies on the refined scope of the proposals.

(2) Better demonstrate the proportionality of the proposed measures and further clarify the content of the options. Given that many Member States have already taken action to implement network and information security measures, the report should strengthen the justification as to why cooperation between them can only be achieved by regulatory intervention. While the report is now clearer on the sectors to be covered by the proposals, it should still provide more detail on the content of the options, in particular for the preferred option and better explain how this will work in practice. For example, more information should be provided on the requirement for organisations to 'adopt appropriate and proportionate measures to dimension the actual risks'. The report should better explain why other possible combinations of 'soft' and 'regulatory' approaches were not considered apart from simply combining options 1 and 2.

(3) Better assess impacts. The report should strengthen its assessment of significant potential impacts which are currently not still adequately addressed, including social/employment impacts, competitiveness, data protection and international aspects. Furthermore, the report should provide a more detailed breakdown of the impacts across the sectors to be affected e.g. health and local authorities. While the report now provides a more detailed analysis of the costs it should strengthen this by including estimates on the likely costs of enforcement of compliance. The report should try to quantify the possible benefits, or at least assess the magnitude of the avoided NIS incidents and of the improved level of security. Moreover, it should clarify whether the likely benefits would outweigh the significant overall costs (for businesses, Member States and public administrations).

Some more technical comments have been transmitted directly to the author DG and are expected to be incorporated in the final version of the impact assessment report

(D) Procedure and presentation
A public consultation has been carried out since the Board's first opinion. The report should provide a summary analysis of the responses to that (in an Annex) and should also clarify the questions that were asked. It should also clarify if Member States' authorities contributed to the consultation. Furthermore, while the detailed information provided in the Annex is an improvement, the report should provide a summary table of all costs and benefits per option within the main text. The report should include an operational evaluation plan.

(E) IAB scrutiny process	
Reference number	2012/INFSO/003
External expertise used	No
Date of IAB meeting	Written procedure The present opinion concerns a resubmitted draft IA report. The first opinion was issued on 6 July 2012

Ref. Ares(2012)824444 - 06/07/2012

EUROPEAN COMMISSION
Impact Assessment Board

Brussels,
D(2012)

Opinion

Title **DG CONNECT - Proposal for a Regulation of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union**

(draft version of 13 June 2012)*

(A) Context

This impact assessment focuses on Network and Information Security (NIS) across the EU. It aims at identifying appropriate measures to improve the level of preparedness and enhance cooperation, coordination and information exchange in the area of NIS amongst the Member States and between market operators and the Member States. Under Article 4(c) of Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency (ENISA): "network and information security" means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

(B) Overall assessment

The report needs to be substantially improved in several respects. First, the nature, scope and scale of the problems should be clarified. In particular, the report should explain why existing measures and mechanisms for NIS are deficient and what precisely the gaps that need to be addressed are. The report should much better demonstrate the cross-border nature of the problem and better explain the weaknesses in private sector preparedness, differentiating between sectors and actors. Second, it should much better justify the proportionality of imposing measures, including costs, across a wide range of sectors and on Member States. Third, the report should clarify the content of the options, explaining what obligations will be imposed and on whom. It should explain how precisely the preferred option in particular will address the problems. Fourth, the report should significantly strengthen its assessment of social impacts, impacts on SMEs/micro entities, competitiveness and international aspects. Fifth, it should give a more detailed assessment of the costs for Member States and affected sectors and a better explanation of the underlying assumptions. Finally, the report should clarify the nature and extent of the external consultation and the views of stakeholders on all key points should be integrated into the text. In the event that no public consultation was carried out, the reasons should be explained.

Given the nature of these concerns, the IAB requests DG CONNECT to submit a revised version of the IA report on which it will issue a new opinion.

* Note that this opinion concerns a draft impact assessment report which may differ from the one adopted

(C) Main recommendations for improvements

(1) Strengthen the problem definition. The problem definition section should be redrafted so as to clarify the nature, scope and scale of the problems. It should much better explain the linkages between these problems and the range of initiatives already taken or underway, including existing legislative requirements. The report should better explain why, despite all the initiatives undertaken so far, it is considered that existing NIS capabilities and mechanisms are overall insufficient. There should be a better explanation as to what has worked so far and what the gaps that need to be addressed are. The report needs to better demonstrate why a strengthened common approach to planning for security attacks is needed across MS, and should make a better effort to show the cross-border effects including by strengthening the evidence base. The nature of the problems should be clarified i.e. why there are gaps in the level of preparedness of some Member States, why there is an apparent lack of trust and what precisely are the problems concerning private companies e.g. apparent lack of adequate investment in security and risk management. There should be a deeper discussion of the nature of the risks including the extent to which, and how, networks and/or services may be affected. In relation to the scope, the report should explain much earlier in the text the range of companies/sectors that are affected in terms of NIS capabilities and should clearly demonstrate, with supporting evidence, the specific weaknesses that need to be addressed, including by SMEs and micros. The report should integrate stakeholders' (different) views on all key aspects of the problem definition.

(2) Better demonstrate the proportionality of the proposed measures and establishment of a clearer intervention logic. Based on a revised problem definition the report should much better justify why it is necessary to impose regulatory obligations to improve NIS mechanisms in Member States and why, in light of the various mechanisms already in place it is necessary to strengthen cross-border cooperation by means of a regulatory approach, particularly for Member States that already have a good level of preparedness. Furthermore, the report should in particular better justify the imposition of regulatory requirements and costs in relation to NIS across a wide range of sectors and actors including on SMEs and micros. The report should strengthen the intervention logic by clearly connecting the problems, objectives and the policy options and in particular by showing how precisely the preferred option will tackle the underlying problems of lack of trust, national level preparedness, cross-border cooperation and inadequate private sector readiness.

(3) Better present the content of the options. The description of the options should better explain what each option implies and exactly what obligations will be imposed and on whom. The report should better explain why a combination of options, based on substance rather than legal form (e.g. a combination of elements of the 'soft' and regulatory approaches) was not considered. In relation to the scope of the obligations, the report should much better explain why it is intended to cover a wide range of additional sectors (information society services sector and the 'regulated markets', banking, finance, energy and transport).

(4) Better assess and compare impacts. The report should strengthen its assessment of significant potential impacts which are currently not adequately addressed, including social/employment impacts, impacts on SMEs/micros, competitiveness, data protection and international aspects. A more differentiated assessment of impacts across Member States (or categories of Member States, depending on the current levels of preparedness) should be provided. Furthermore, the report should provide a more detailed breakdown of the impacts across the sectors to be affected (information society services, banking,

energy and transport). A more detailed assessment of the costs on Member States and private companies should be provided, including a better explanation of the underlying assumptions. While the report provides an estimate of the cost per company it should also include an assessment of the total number of private and public organisations affected and the total costs of the measures.

Some more technical comments have been transmitted directly to the author DG and are expected to be incorporated in the final version of the impact assessment report

(D) Procedure and presentation

The report should clarify the nature and extent of the external consultation and whether a dedicated public consultation was undertaken. It should clarify what questions relating to the issues at hand were put to public consultation and what the responses of stakeholders were. The (different) views of stakeholders on all key points should be integrated into the text including notably on the scale/nature of the problem, the options and their impacts.

(E) IAB scrutiny process	
Reference number	2012/INFSO/003
External expertise used	No
Date of IAB meeting	4 July 2012