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