



EUROPEAN COMMISSION
IMPACT ASSESSMENT BOARD

Brussels, 27 AVR. 2010
D(2010)

Opinion

Title **DG INFSO - Impact Assessment accompanying the proposal for a regulation of the European Parliament and the Council on a modernised Agency for Network and Information Security**

(Resubmitted draft: version of 15 April 2010)

(A) Context

The European Network and Information Security Agency (ENISA) was established in 2004 for an initial period of five years, with the main goal of ensuring a high and effective level of network and information security within the Community. In September 2008, the mandate of ENISA was extended, unchanged, for 3 years, and the European Parliament and the Council called for "further discussion about the Agency [and] the general direction of the European efforts towards an increased network and information security". This impact assessment accompanies the proposal for a modernised Network and Information Security Agency.

(B) Overall assessment

While the impact assessment has been improved on a number of issues - in particular the methodology for the assessment of impacts has been revised - there remain areas where further clarifications are needed. The report should provide further details on why the functions and mandate of ENISA do not correspond to the current network and information security environment. It should then clarify how the mandate of the modernised Agency will be designed to allow the Agency to respond flexibly to the evolving network and security environment. The report should develop further the presentation of the preferred option by strengthening the link between actions foreseen under this option and the problem drivers identified. Finally, the assessment of international impacts and impacts on the fight against cyber crime should be strengthened.

(C) Main recommendations for improvements

(1) Provide further details about the current functions and mandate of ENISA and explain how the mandate of the modernised Agency will be adapted to constantly evolving NIS environment. While the report states that ENISA's mandate is limited and does not correspond to current network and information security environment, it should provide further details to substantiate this statement, and briefly summarise which tasks are conferred to ENISA. It should, for example, explain clearly that under the current mandate ENISA cannot: support the networking of governmental CERTS (2.2.2); develop the data collection framework (2.2.3); contribute to cooperation with third countries (2.2.5) etc). The report should then explain how proposed changes to the mandate will overcome the inefficiencies and rigidities of the current mandate. In particular, it should clarify what other changes - in addition to expanded functions and increased resources of the Agency - would allow the Agency to react appropriately to evolving network and security challenges. The report should clarify whether changes of organisational structure are foreseen.

(2) Be clearer about the content of the preferred option and how it deals with the problem drivers. The report should strengthen the link between option 3 and the problem drivers identified. It should in particular explain more clearly in section 5 which activities of the modernised Agency are foreseen to address the diversity and fragmentation of national approaches (2.2.1), the international dimension of NIS problems (2.2.5), and the need for more efficient fight against cyber crime (2.2.7).

(3) Strengthen the assessment of international impacts and impacts on the fight against cyber crime. The revised report provides an overview of the main expected impacts and assesses them qualitatively. This seems more appropriate than the scoring method previously used. The assessment of international impacts should however be strengthened, by explaining better the extent to which the proposed option would enhance international cooperation and coordination of network and security related issues. In addition, the report should assess further the impact of new non-operational tasks of the modernised Agency on the fight against cyber crime.

(D) Procedure and presentation

Following the previous Board recommendations, the executive summary has been updated and now presents the main impacts of options and broadly outlines the monitoring and evaluation arrangements. Annex 12 summarising the evaluation results has been added. While the positions of the stakeholders are better integrated into report, the extent to which these positions are representative should be clarified. Further efforts could be made to bring the report closer to the recommended length of 30 pages, e.g. by shortening sections 2.7 or 3.3.

(E) IAB scrutiny process	
Reference number	INFSO/2010/020
External expertise used	No
Date of Board Meeting	Written procedure The present opinion concerns a resubmitted draft IA report. The first opinion was issued on 26 March 2010.