EUROPEAN COMMISSION

Brussels, 17.9.2013
C(2013) 5878 final

Dear President,

The Commission would like to thank the Riksdag for its Reasoned Opinion on the Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security ("NIS") across the Union {COM(2013) 48 final}.

The Commission does not share the view of the Riksdag that the proposal does not comply with the principle of subsidiarity. As explained in detail in the Impact Assessment accompanying the proposal, the European Union intervention in this area is justified because the impact of many incidents transcend national borders and undermine the functioning of the internal market. The Commission has so far pursued a voluntary approach, by calling on Member States to have adequate NIS capabilities and to cooperate on countering cross border incidents, and by calling on industry to better manage risks and invest in security solutions. However this approach has not been able to overcome an uneven level of preparedness and limited cooperation across the EU. For instance only 10 Member States are part of the European Government CERTs (EGC) group. Non-intervention at EU level would lead to a situation where some Member States would continually lag behind in terms of preparedness and response, which would weaken the overall level of NIS across the EU given the interconnectedness of the various networks and systems. Member States are also starting to introduce their own regulatory requirements for risk management and incident reporting in an uncoordinated manner, which generates internal market barriers in terms of additional administrative burdens and compliance costs for companies operating in more than one Member State. Many replies to the Commission's public consultation stressed the burden created by the absence of a truly integrated market and harmonised regulatory requirements. This also has a disrupting impact on the provision of cross-border services which can become unavailable, suspended or interrupted due to security breaches. As mentioned in the Impact Assessment, in January 2011, the Commission had to suspend the Emissions Trading System due to security breaches at national registries, which prevented companies from selling and buying emission allowances within the EU. eBay and PayPal have experienced web-based attacks that made all or portions of their websites unavailable for periods of time in 2010, thereby affecting e-commerce in the internal market.

Mr Per WESTERBERG
President of the Riksdag
SE – 100 12 STOCKHOLM

In preparing its proposal, the Commission gave special consideration to the principle of proportionality. The requirements for the Member States are set at the minimum level necessary to achieve adequate preparedness and to enable cooperation based on trust. This also enables Member States to take due account of national specificities and ensures that the common EU principles are applied in a proportionate manner.

For example, Chapter II of the proposal gives Member States the freedom to define the tasks of the competent authority and the CERTs. The proposal also leaves Member States enough flexibility to decide on the structure of these entities: Article 6 of the proposal does not require the NIS authorities to be independent, and under Article 7 the Member States are free to set up a CERT within or outside the competent authority.

At European level, the network set up under Chapter III is a cooperation mechanism with no legal personality. The possibility to cooperate at EU level on incidents having a cross-border dimension should not in any away be detrimental to rapid reaction at local level.

Concerning the rules for market operators in Chapter IV, both the scope and the substantive obligations on market operators are limited. As regards the scope, only providers of critical infrastructure are covered, while micro enterprises are excluded. As the list in Annex 2 is not exhaustive, Member States are free to determine the precise scope and nature of market operators at national level. As regards the substantive obligations, the proposal does not impose any precise security measures but provides for general risk management and information provision requirements. To avoid imposing a disproportionate burden on small operators, the requirements are proportionate to the risk faced by the network or information system concerned.

The costs of the proposal on both Member States and market operators are described in the Impact Assessment. The Commission believes that they are not excessive, considering what is at stake, and are likely to be outweighed by the overall economic and social benefits. For instance, based on the calculations in the Impact Assessment, the Commission estimates that the average compliance cost for an SME would be between 2500 - 5000 EUR, while currently available private data on the average cost of an SMEs most serious security breach ranges between 41 000 - 77 000 EUR[1]. The cost of non acting is thefore substantial. And a coordinated approach at EU level will limit the costs on operators, who may otherwise have to comply with differing or conflicting national requirements.

The Commission hopes that these clarifications address the points raised by the Riksdag and looks forward to continuing this dialogue in the future.

Yours faithfully,

Maroš Šefčovič
Vice-President

[1] http://www.pwc.co.uk/audit-assurance/publications/2013-information-security-breaches-survey.jhtml