

Brussels, 5 June 2014

Dear Minister,


The American Chamber of Commerce to the European Union (AmCham EU) has consistently supported the EU's efforts to improve cybersecurity preparedness and resilience and to foster public-private trust and cooperation. Indeed building trust and security are of paramount importance for our members. We welcomed the Council's support for the European Cybersecurity Strategy¹ and we also see the European Parliament's first reading vote on the Commission's proposed Network and Information Security Directive as a very encouraging and positive step forward.

We believe that the Council should examine in some detail the issues at stake in the proposed Directive. In particular the Parliament amendments on scope, effectiveness of mandatory reporting and liability are important. We fully support these as they focus the scope of mandatory reporting to significant incidents disrupting the core services of critical infrastructure operators. However, AmCham EU is concerned that the objective of creating a level playing field for market operators in Europe may have been lost from sight in the Council. As a cross-sectoral trade association representing over 150 companies active in all EU Member States, this would be an important achievement. If trust and cooperation are to be built between the public and private sectors, market operators need legal clarity and certainty as to what requirements will be applicable to them, where, on what basis, under what conditions, with what incentives and safeguards. The current Council proposals are very far from that mark, as they would allow excessive fragmentation and divergence through national implementation.

We call on the Council to reconsider this approach. While we understand that national sovereignty considerations and the subsidiarity principle that govern national cybersecurity strategies, cyber capability building and intergovernmental cooperation in this field, we believe that these considerations can and must be reconciled with a much more ambitious level of harmonisation of the chapter relating to market operators, in particular as regards the scope definition and the incident reporting rules. Given the intrinsically crossborder nature of cyber threats facing Europe and the international dimension of many market operators concerned, we believe that common rules harmonised across the internal market are the necessary minimum to meet the shared objective of heightening the level of cybersecurity across the EU.

We urge you to consider these concerns seriously before committing to an approach that might eventually fail to deliver the results we all expect.

Yours sincerely,



Pastora Valero
Chair, Digital Economy Committee, AmCham EU

¹ Council Conclusions of 25 June 2013.