Brussels, 4 August 2017

**BSA feedback on European Commission 'inception impact assessment' on the 'Proposal for a Regulation revising the ENISA Regulation (No 526/2013) and laying down a European ICT security certification and labelling framework'**

BSA | The Software Alliance (BSA), the leading advocate for the global software industry, welcomes the opportunity to comment on the European Commission's inception impact assessment on the 'Proposal for a Regulation revising the ENISA Regulation (No 526/2013) and laying down a European ICT security certification and labelling framework.' BSA commends the Commission for the steps it has taken to strengthen the EU's cyber resilience and shares the desire to continue building trust in the Digital Single Market. As the Commission further develops possible policy options related to both the review of ENISA's mandate and the potential creation of a European ICT security certification and labelling framework, we wish to provide the following comments:

BSA is a strong supporter of ENISA and believes the agency has played a central role in strengthening the capability of Member States and industry in preventing, detecting and responding to cyber threats and incidents. We encourage the Commission to renew the mandate of ENISA and support "Option 2 – Enhanced ENISA", ensuring that ENISA plays a central role in facilitating the exchange of cross-sectoral best practices, particularly when it comes to adoption of baseline 'cyber-hygiene' techniques. Moreover, ENISA should have a larger role in developing cooperation with third countries as the cyber threat landscape is global in nature and thus requires international solutions.

While we support the work of ENISA, we would caution against "Option 3" as we see no need for ENISA to obtain full operational capability, particularly when it comes to the development of EU wide standards or the implementation of potential security certification and labelling frameworks. Incident mitigation and response should remain the competence of national Computer Security Incident Response Teams (CSIRTs). Instead, ENISA should focus on further supporting CSIRTs through cyber exercises aimed at increasing cross-border cooperation for responding to large scale cyber incidents.

On the issue of certification and labelling, we encourage the Commission to pursue "Option 1", with a strict focus on voluntary, consensus-based, and industry-led initiatives including self-assessment schemes. BSA believes that such a process should rely upon international standards and welcomes the recognition by the Commission of this important facet in its roadmap. Moreover, BSA members would be open to the contribution of ENISA's technical expertise in the development of any technical specifications and standards, in the context of on-going international efforts.

However, relying upon a voluntary, consensus-based, and industry-led standard setting process cannot be an effective approach unless the approach is adopted on a wide scale. Market-driven incentives for adopting any future standards are preferable to other alternatives - requiring

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

adoption through legislation or using adoption to shape insurance markets and legal liability may have the unintended result of impeding flexible, outcome-oriented standards. Instead, industry and the Commission must collaborate to develop incentives for adoption. This will require any future certification schemes to emphasize security development lifecycle (SDL) processes to be flexible and outcome orientated. There must also be an alignment amongst approaches as a proliferation of different initiatives will serve to confuse rather than inform end-users.

We also support the Commission in encouraging more Member States to join SOG-IS. However, we caution against pursuing this through a legislative proposal making Member State participation mandatory as SOG-IS participation is closely linked to available Member State resources. Instead, it should be encouraged with an emphasis placed on resource and capacity building. Furthermore, we note that SOG-IS cannot become a 'catch-all' solution as it is specifically tailored towards 'Common Criteria' and this approach cannot apply to most software products.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48