Gooimeer 4-15
1411 DC Naarden

088-1182510
Info@cyberveilignederland.nl

European Commission
DG for Communications Networks, Content and Technology
CONNECT.H Digital Society, Trust & Cybersecurity
Mrs. Lorena Boix Alonso B-1049 Brussels,
Belgium

Response to European Commission Public Consultation on the Cyber Resilience Act

Naarden, 25-05-2022

We appreciate the opportunity to respond on behalf of Cyberveilig Nederland, the association of the cybersecurity sector in the Netherlands, to the European Commission Public Consultation on the Cyber Resilience Act.

Cybersecurity is essential for a digital society
Our societies within the EU are highly digitized and connected. This offers many opportunities for the social and economic challenges facing the EU. Unfortunately, this makes us also vulnerable for cyber incidents. Therefore, we see the need for common standards to improve the cybersecurity for products in the European internal market, as stated by the European Commission. Cyberveilig Nederland, the association of cybersecurity companies in the Netherlands, agrees with the importance that all the digital products, processes and services must be trusted to be digitally secure. Therefore, we would welcome the upcoming Cyber Resilience Act (CRA). However, Cyberveilig Nederland would like to give some points of attention:

- The focus of the CRA should be on setting cybersecurity requirements that covers all forms of both digital products and services, irrespective if they are offered for consumer or business/industrial purposes and irrespective if they are linked to a physical product. However, critical infrastructures require different cybersecurity safeguards than home-computing applications or simple office environments. Striking a balance between these different fields is complex and asks further elaboration of the CRA.

- The level of security for software products is higher in almost all phases. A lot of hardware related security only occurs at a very late stage of development, and the possible flaws are complex to solve once the product is in use. Therefore, the CRA should cover the entire lifecycle of digital products, processes and services through a duty of care based on the latest state of technology.

- A risk based approached is necessary to increase cybersecurity in businesses, public administrations and for consumers using digital products and services. Therefore, the CRA should not be focussed on solely technical security. Effective cybersecurity is a combination of technique, organisation and the human factor.

- More and more digital attacks are taking place in the supply chain (e.g. SolarWinds). Many manufactures of hard- and software are located outside the European Union. How will the CRA do to hold these organisations accountable for their responsibilities?

- Various (cybersecurity) regulations are currently under development (NIS2.0, Cybersecurity Act) that foresee in a digital resilient EU. How will the EC ensure that these regulations reinforce and are aligned each other?

- Trust services or critical infrastructures require different cybersecurity safeguards than home-computing applications or simple office environments. The cybersecurity maturity level varies widely and also the self-reliance differs enormously.

To summarize, the discussion about the need and content of a Cyber Resilience Act could provide an opportunity to harmonize European cybersecurity obligations and achieve more legal consistency between national and European levels. We also welcome the objective of setting up a level playing field for vendors. Promoting the cybersecurity of products will help to mitigate potential vendor losses and have a positive effect on the economy and innovation in the EU. Therefore, Cyberveilig Nederland welcomes the CRA.

We would be pleased to have further dialogue with the European Commission and to discuss any comments or questions you may have regarding our responses. We can be reached as follows:

Petra Oldengarm, director (petra@cyberveilignederland.nl)
Liesbeth Holterman, strategic advisor (liesbeth@cyberveilignederland.nl)

Yours sincerely,

Liesbeth Holterman
Strategic advisor Cyberveilig Nederland

About Cyberveilig Nederland.
We are committed to creating an optimal entrepreneurial climate for cyber security firms in the Netherlands. We introduce transparency in the sector through the development of a conduct code and certification hallmark. We actively participate in the public debate and see cyber security not only as a risk, but rather as an opportunity to position the Netherlands as a country that provides safe products and services. We engage the authorities and other strategic partners to implement our knowledge and expertise of cyber security in the work field for the greater good. We initiate partnerships between cyber security firms themselves and we also bring users and suppliers together. We are in discussion with the government and political leaders in order to remove (future) bottlenecks that may obstruct the digital resilience of the Netherlands. All of these aspects ensure that we enhance our visibility in and our impact on our sector.