BlackBerry, the global cybersecurity software and services company, welcomes the opportunity to provide feedback on the Commission's proposed Artificial Intelligence Act. We welcome efforts by public authorities to promote the development and deployment of secure and innovative AI systems.

We support the proposal's risk-based approach and would recommend maintaining this as it advances through the legislative process. We believe that the proposal could be strengthened, however, if "high-risk AI" were more precisely defined, to include a discussion of how product- or system safety components are integrated into this definition. For example, the formulation "AI system itself as a product" in Article 6 (b) does not clarify if the product is a safety product or to what products the article is refereeing to. The definition should also account for the fact that an AI system may be high-risk or non-high-risk depending on the context in which it is used.

We strongly support adopting an AI framework which introduces different obligations for AI providers and AI users thus achieving greater proportionality and fairness. Additional clarifications on the criteria for non-safety AI components used in automotive and radio equipment, as well as on terms such as "placing on the market", "making available on the market", "putting into service", or "reasonably foreseeable misuse" would also help.

As an alternative to the redress and enforcement provisions, we would welcome the introduction of mechanisms that incentivize the integration of AI systems into public sector and enterprise environments and that meet the compliance criteria laid down by the proposal. Such an approach could help create a market uptake of approved AI systems that will benefit Europe's digitization, ultimately promoting cybersecurity, which relies on AI automation, including for incident prevention, detection, mitigation and response.

Regarding the interaction of the AI Act with other horizontal or sectoral legislation, further clarity would be helpful to delineate where the requirements for high-risk AI and components used by critical utility infrastructures (as defined under Annex III.2.a) apply. As an example, the NIS Directive review sets risk management and incident reporting requirements for SaaS software (including AI-powered software and applications) and for critical operators. It is important to minimize overlaps and regulatory redundancy with existing rules, particularly regarding elements such as information security management, technical assessments, conformity or compliance. With regard to AI systems regulated under legislation listed in Annex II, the compliance process should account for the latest international arrangements to which the Union is a signatory, including those that introduce new sectoral requirements, such as the update of EU regulation 2019/2144 including for the provisions introduced by UNECE Regulations No. 155 and 156.

Concerning Article 40 on Harmonized standards, we recommend that the European Commission participate in international standards development organizations or European Standards Organizations (ESOs) to set clear requirements for the standards to support the AI Act, as the SDOs or ESOs are progressing in AI standards development. We urge CEN/CENELEC to consider introducing more open and transparent standardization processes to obtain more broad inputs and feedback. A good example to follow is Industry Specification Groups (ISG) of ETSI in which non ETSI member can participate.

We welcome the opportunity to achieve cybersecurity conformity through a cybersecurity certification scheme as proposed under Article 42(2), to the extent that it remains voluntary and other conformity methods are also foreseen to achieve compliance. Furthermore, we would welcome additional guidance from the Commission and ENISA as to which existing schemes (or schemes under development, or future schemes to be introduced by the Union Rolling Work Program) would meet cybersecurity requirements of AI systems. To best support global convergence and the ability of EU players to compete globally, conformity processes should account for widely adopted international standards.

We look forward to further engaging with the Commission and the co-legislators to support the adoption of an AI regulation underpinned by the ‘better regulation’ principle and benefiting from relevant expert stakeholder input.