Statement from the Charter of Trust

The Charter of Trust welcomes the opportunity offered by the Australian Government to provide feedback on the discussion paper *Strengthening Australia's cyber security regulations and incentives*. We are pleased to see that the Government of Australia and the Charter of Trust are following a similar path, namely that of making the most of cybersecurity and the standards it can set in order to improve the resilience of digital economies.

Since 2018, the Charter of Trust has been working towards building trust in cybersecurity by advocating for the right kind of regulation. This open consultation is therefore a much-valued opportunity for the Charter to express its views on how businesses can be incentivised to invest more in cybersecurity risk management.

Regarding Chapter 4 *Governance standards for large businesses*, Charter of Trust Partners believe that the best approach for strengthening corporate governance of cyber security risks would be to **incentivise businesses through a balance of voluntary and mandatory measures from government.** This should follow a **risk-based approach**, i.e. voluntary cross-sector baselines that could be established for lower risk levels, and sector-specific mandatory requirements for higher risk levels. This would ensure complete adoption of cybersecurity principles and standards and strengthen the cybersecurity posture of companies, while enabling them to leverage the benefits of both voluntary and mandatory organizational and technical requirements and associated demonstration of assurance.

Within the framework of the Charter of Trust's 10 Principles, we have successfully established cybersecurity maturity level benchmarks as well as supply chain and security-by-default baselines. These are absolute baseline requirements which can be adopted across different industries. The Charter's Partners, all of them large and global corporations, have adopted and implemented these baseline requirements according to their business needs and risk assessment, which have proven to effectively reduce cybersecurity risks.

We believe that horizontal mandatory cyber security regulation would be difficult to implement for all risk levels within relevant timeframes and because of the cross-sectoral nature of the approach and because of the lack of resources that this would cause, leading to a diluted effort. It would be difficult for binding regulation to unfold its potential equally across industry sectors. Regulatory requirements should be harmonized to avoid overlapping requirements for providers. The Charter of Trust serves as an example that voluntary commitments, on the other hand, allow for the flexibility needed to **maximize adoption and implementation of important cybersecurity baselines** regardless of the nature of an enterprise.

With the active work done by the Charter of Trust's Principle Taskforces, we have some more specific views to offer:

Principle 1 – Ownership for cyber and IT security

In Principle 1 the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and roles in the organisation is anchored. The assessment of risks through clear Key Performance Indicators (or the equivalent), quantified management measures, targets and reports as well as the right mindset throughout organizations – "It is everyone's task" – have to be established.

Principle 2 – Responsibility throughout the digital supply chain

The Charter of Trust proposes a **risk-based approach** derived from international standards. There is no one fits all solution, and there are too many individual requirements from companies, industries, regulations and so on. By establishing our 17 Baseline Requirements for Principle 2, we set a basic level of cybersecurity for every supplier, by which companies can demonstrate a certain maturity~~.~~ Combined with an appropriate verification according to risk, we define the foundation of cybersecurity development at a large scale and ensure significant synergies among industries and regions. We share our knowledge and ideas, e.g. in the form of whitepapers.

Principle 3 – Security by default

Principle 3 focuses on the adoption the highest appropriate level of security and data protection and ensuring that it is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures, and business models. This principle has put together cybersecurity baseline requirements and explanatory documents to ensure security by default across industries. These requirements are also verifiable, thereby ensuring a successful adoption.

Principle 6 – Education

The Charter of Trust requests to include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education, and trainings – in order to lead the transformation of skills and job profiles needed for the future.

Principle 7 – Certification for critical infrastructure and solutions

Where "life and limb" is at risk (based on future-proof definitions in particular) for critical infrastructure as well as critical IoT solutions, governments working closely with industry should establish mandatory independent third-party certifications for such high-risk environments.

Principle 8 – Transparency and response

Charter of Trust members have developed a voluntary threat intelligence sharing cluster between members in order to share new insights, indicators of compromise affecting different sectors. This uses the widely known Traffic Light Protocol to amber level to ensure the right kind of information is shared with regard to confidentiality.

The Charter of Trust appreciates the opportunity to provide input to your consultation and would be pleased to provide further detail on any points we have raised in this document.