IBM Australia Limited
259 George Street
Sydney, NSW 2000

IBM Australia
28 Sydney Ave
Forrest, ACT 2603

29 April 2021

The Productivity Commission
Contact Officer: Yvette Goss
Vulnerable Supply Chains
Supplychains@pc.gov.au

Dear Commissioners Catherine de Fontenay and Jonathan Coppel,

Re: IBM Submission and comments to inform the Vulnerable Supply Chains Final Report.

Thank you for the opportunity to submit a response to the Productivity Commission Interim Report on Vulnerable Supply Chains in Australia. IBM is uniquely positioned to share our perspective developed through our work with supply chains for essential goods and services including key Government departments, critical infrastructure organisations and the broader market.

The interim report highlighted the network-like nature of a supply chain, using an analytical framework that assesses inputs like labour, services, and capital. IBM believes the current report could be enhanced by considering potential vulnerabilities relating to technology and policy implications as a result of this.

- **Cyber-security should be highlighted as the biggest risk to Supply Chain productivity.**

  Part of the challenge is that there is no single, functional definition of supply chain security and mitigating this risk is a moving target and mounting challenge. Supply chains are increasingly complex global networks comprised of large and growing volumes of third-party partners who need access to data and must provide assurances they can control who sees that data. Further challenges are introduced by today's constraints on staff, budgets, rapid unforeseen changes to policy or geopolitics, partner strategies and the supply and demand mix.

  Noting that the top seven essential industries being supplied to Australia are also named in the Security Legislation Amendment (Critical Infrastructure) Bill 2020 ("SOCI") this interim report only makes cursory mention of both cyber-attacks (as an infrastructure-related risk) and broader technology implications. This is a significant gap. The report does mention some technology implications however these are limited to IoT and cyber-risk. Widespread situational awareness across supply chain elements is needed so that any vulnerabilities are quickly discovered and remediated, and any consequences of exploitation be detected as soon as possible. Whilst there are initial elements of this emerging as part of the Federal Government 2020 Cyber Security Strategy, recognising that such models can be applied across supply chains is recommended.

  Security should not be seen as a separate consideration to any of the technology or infrastructure concerns above, but as overall embedded 'security by design' across the supply chain network. This ensures that the value chain can remain secure at all points and can continue to benefit and avoid disruptions of a cyber nature. In particular, solutions are beginning to incorporate artificial intelligence to proactively detect suspicious behaviour by identifying anomalies, patterns and trends that suggest unauthorised access. For example;
  - AI-powered solutions can send alerts for human response or automatically block malicious attempts;
  - Blockchain ecosystem Farmer Connect transparently connects coffee growers to the consumers they serve, with a blockchain platform that incorporates network and data security to increase trust, safety and provenance; and
  - One of the busiest seaports in the world Port of Los Angeles is building a first-of-its-kind Cyber Resilience Centre with a suite of security offerings aimed at enhancing its supply chain ecosystem's awareness and readiness to respond to cyber threats that could disrupt the flow of cargo.

These critical supply chain initiatives demonstrate the 'security by design' approach and ensure that risk management is a key factor in the supply chain enabled by technology. It's critical that this risk management approach considers all elements of the supply chain, so that maturity can rise equally and therefore limit opportunities for adversaries to exploit any link in the chain.

- **Infrastructure needs to give greater attention to how emerging technology is mutually exclusive to IT Systems.**

With a focus on maintaining supply chain productivity, Australia cannot afford to simply 'react' to another 'black swan' event (e.g., another pandemic). Whilst technology investment is inevitable to drive resilience and transparency, this topic should be considered from two capabilities: becoming Cognitive (adopting a level of AI, Blockchain, IoT and Automation maturity); and on the Cloud (embracing a combination of Public, Private and Mainframe modernisation).

Supply chain workflows are ideal to leverage AI, Blockchain, IoT and Automation to reach new levels of responsiveness. These workflows challenge siloed processes allowing supply chains to work as a consortium rather than individual partnerships.

Taking Figure 2.2 from the report and reconceptualising it as a cognitive workflow, supply chains could leverage data from IoT sensors which uses an AI model to ensure that certain country requirements allow for a view on whether suppliers from raw to processed materials satisfy other needs. If countries have the ability to understand which suppliers should be avoided (red) versus which ones would be safer (green) thus using data to better inform decision making, all through the power to becoming a cognitive enterprise.

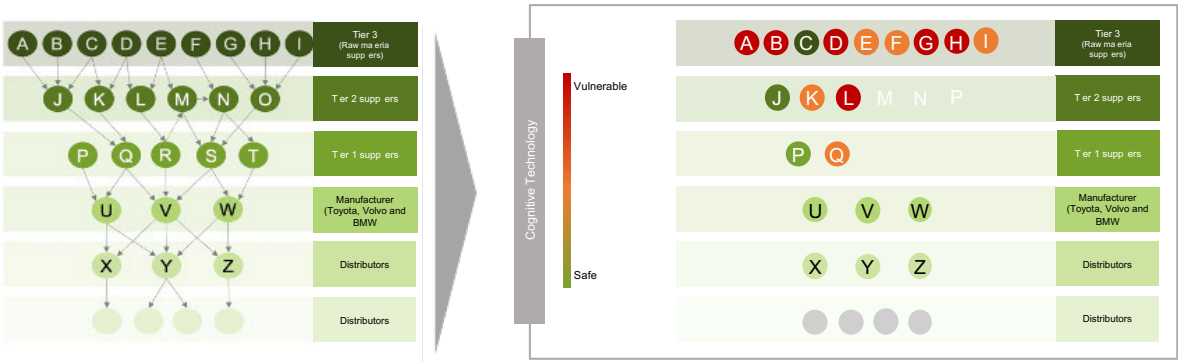

Figure 1 (based on Figure 2.2 of the Report)– Evolution of the firm-level supply chain from Chandra and Kamrani (2004, p. 573) to consider the benefits possible as a cognitive supply chain.

From the identification, assessment and addressing of potential disruptions, to be able to mitigate the impact of unpreventable disruption, technologies like AI and IoT can simulate process-optimization scenarios and provide instant shipment quoting capabilities that reflect actual market rates with two important examples are seen through IBMs work with Food Trust. This allows for pandemic scale events to be less reactive.

Although the interim framework considers that breaks to a supply chain will only be driven in similar black swan events or entire brand or component failures, any step of the chain provides an opportunity for transformation from demand planning, to manufacturing execution, or order orchestration and fulfilment is critical to uncover any level of a new transparency.

- **Risks should account for more than firm & market - to not limit policymakers' ability to appreciate technology-based implications to both economic productivity and statutory interpretation**

  Amidst any future pandemic level situations, government workers performing sensitive missions were suddenly working remotely. As governments responded to the crisis, IT systems were heavily stressed by increased workloads. While agency IT leaders accelerated modernisation, systems and networks were still pushed to their limits. This impacted mission-critical operations and in some areas diminished the government's ability to respond to the crisis. The ways that leaders have accelerated modernization during the COVID-19 response have shown that technology needs to enable entirely new ways of operating. Policymakers should reorient and accelerate modernization to transform government IT systems to become Tomorrow Ready. No one knows what the next emergency will be or how specific agency missions will evolve.

  For this reason, Trade Agreements are an essential component in this effort. Indeed, facilitating digital trade and ensuring a safe and secure data economy are not mutually exclusive. For the past decade, negotiators have made significant progress in developing new trade provisions to facilitate cross-border data flows and protect underlying intellectual property, including the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, the US-Japan Digital Trade Agreement, the Digital Economy Partnership Agreement, the US-Mexico-Canada Agreement and the Australian Singapore Digital Economy Agreement

  In parallel, there are renewed efforts to enhance cybersecurity, privacy, and data protection cooperation between governments and the private sector, such as the Data Free Flows with Trust Initiative launched by Prime Minister Shinzo Abe at the 2019 G-20. We welcome these efforts and continued trade policy development that enable Australian markets and firms to be successful.

We appreciate the Commission's consultative approach on this area of concern and are happy to address any of our points in greater depth if you have any questions.

Yours sincerely,

Kylie Watson
Partner, Cyber Security & Cloud Services

Chris Hockings
CTO, IBM Security

Contributors to this response include:
Zuben Rustomjee, *Jasmine Bansal*