CPA Australia Ltd
ABN 64 008 392 452

Level 20, 28 Freshwater Place
Southbank VIC 3006
Australia

GPO Box 2820
Melbourne VIC 3001
Australia

Phone 1300 737 373
Outside Aust +613 9606 9677
Website cpaaustralia.com.au

25 March 2022

Department of Home Affairs
6 Chan St
Belconnen ACT 2617

By email: critical.technology@homeaffairs.gov.au

Dear Sir / Madam,

Submission on the Critical Technology Supply Chain Principles

CPA Australia represents the diverse interests of more than 170,000 members working in 100 countries and regions around the world. We make this submission on behalf of our members and in the broader public interest.

Supply disruptions can have significant consequences for businesses' ability to operate. Resilient supply chains, including critical technologies are foundational to Australia's economic prosperity and security.

To strengthen the Critical Technology Supply Chain Principles' (the Principles) potential to mitigate and manage supply chain vulnerability, we suggest the government considers the following recommendations:

- Principle 2 be amended to "Understand the different security risks posed by your supply chain and develop appropriate risk mitigation strategies."
- Businesses be provided with resources and advice that assists them to better understand their security and supply chain risks and how to implement these principles.
- Traceability be added to the transparency principles.
- A list of existing standards and international benchmarks for suppliers be published and/or template examples of minimum transparency requirements for supply contracts be provided.
- Principle 9 be amended to "Consider if suppliers operate ethically, sustainably, with integrity, and consistently with international law and human rights."
- Principle 10 be amended to "Build strategic partnering relationships with critical suppliers and avoid over-reliance on single suppliers."
- The Government extend its support of further technology pilots focused on improving supply chain security, transparency and traceability as well as sustainability.
- Government consider digital platforms and technology interoperability to improve supply chain resilience and agility.
- The Federal Government launch an initiative to bring together businesses across all sizes to identify supply chain pain points, develop solutions and collaborate.
- Funding for the upskilling and reskilling efforts be significantly increased so that small businesses and workers keep pace with Australia's transition to a digital economy.

CPA Australia's perspectives on these issues are provided in the attachment to this letter.

If you have any questions about this submission, please do not hesitate to contact Dr. Jana Schmitz, Digital Economy Policy Lead at CPA Australia on jana.schmitz@cpaaustralia.com.au.

Yours sincerely

Dr Gary Pflugrath FCPA
Executive General Manager, Policy and Advocacy

Encl.

Attachment

Overall commentary on the principles

We support the adoption of the Critical Technology Supply Chain Principles (the Principles). We believe they uplift the security of Australia's critical technology supply chains and enhance supply chain resilience. We therefore urge federal and state governments to take steps to encourage businesses to implement these Principles.

If, after an appropriate period, Australia's critical technologies supply chains remain unacceptably vulnerable due to low levels of implementation of the Principles, the government should initiate a further consultation on whether such principles should be mandated and what businesses would be subject to such a mandate.

We suggest that the Principles undergo periodic reviews to ensure they remain fit-for-purpose and relevant in the rapidly changing digital economy. As part of such reviews, "best practice" examples and case studies should be added and/or updated.

We also suggest that the Department of Home Affairs initiate regular stakeholder engagement on the Principles. This would ensure that issues can be identified and addressed quickly.

The Three Pillars

Security-by-design

We agree that cyber security needs to be recognised as a high priority for all supply chains participants, especially at points that must not fail.

The pandemic, climate disasters and geo-political tensions have exacerbated the threats to and potential fragility of global critical technology supply chains. In Australia, this has heightened the need for domestic capacity and capability and the implementation of secure-by-design principles into supply chain management and critical technologies.

While we support the intention of *Principle 2*, we doubt that "understanding" different security risks offers sufficient protection from supply chain risks. We suggest that Principle 2 be amended to emphasise risk prevention and risk mitigation.

Recommendation 1:

Principle 2 be amended to "Understand the different security risks posed by your supply chain *and develop appropriate risk mitigation strategies.*"

Businesses are better able to identify and monitor potential security risks if they group contracts or suppliers into different risk profiles, based on considerations such as:

- impact that loss, damage or disruption has on business operations
- nature of the service suppliers are providing
- type and sensitivity of information suppliers are holding / processing etc.

Each risk category will require slightly different treatment and handling to reflect the associated risks. It is important to review the identified risks periodically as changes to supply chains can occur internally and externally at any time.

Our research shows that small- to medium-sized entities (SMEs) are particularly prone to security risks. These views have been confirmed by the Australian Securities and Investments Commission (ASIC), which reportedly states that "the greatest gaps between large firms and SMEs are in supply chain risk management, cyber intrusion monitoring and detection, and recovery planning".[1] ASIC notes that it did not see material improvements in supply chain risk management between 2018-19 and 2020-21. We recommend that the government supports businesses in understanding security and supply chain risks by providing and / or linking to relevant resources.

We support *Principle* 3. However, we suggest that instead of the principle requiring building security measures into "all organisational processes" which involve external parties, it should encourage businesses to focus their attention on critical technologies that allow for the secure engagement with and exchange of information with other relevant supply chain participants.

We support *Principle 4*. Encouraging suppliers to continue improving their security arrangements is crucial. Promoting security within their supply chain is particularly important as cyber-attacks can compromise and infiltrate the supplier's entire network.

Overall, on the Security-by-design principles, we suggest that the government provides case studies, examples and education material elaborating on these principles and explaining how to apply them. Such case studies should include examples of third-party software providers and data storage services.

By way of example, the United Kingdom National Cyber Security Centre (UK NCSC) provides case studies supporting its Supply Chain Security Guidance.

Recommendation 2:

Businesses be provided with resources and advice that assists them to better understand their security and supply chain risks and how to implement these principles.

Transparency (and traceability)

We highlight the importance of supply chain transparency. It promotes awareness of risks of potential shortages, helps identify bottlenecks and assists businesses in determining whether alternative sources of critical inputs are needed.

Supply chain transparency is not only important from a security perspective – it also helps ensure the integrity and quality of products and is vital for entities required to report under the Modern Slavery Act.

Technology-led approaches to supply chain transparency assist organisations reduce the risk that exploited workers are being used in their supply chains and helps assure the origins of these goods and services. These considerations are increasingly important given heightened scrutiny of goods manufactured under potentially exploitative conditions.

We recommend complementing the transparency principle with "traceability". While transparency involves sharing information among different participants across the supply chain network, traceability refers to the ability of the system to identify and verify individual components including the historical state of activities. Traceability applies not only to the physical movement of a product but also to the information related to product origin, quality and safety. This involves tracking a product's flow and its attributes throughout the entire supply network.

Increased transparency and traceability of supply chains will enable companies, consumers, and regulators to better understand the safety, provenance, and sustainability of value chains, amidst the rising demand for more stringent environment, sustainability, and governance standards (see our comments on Principles 9 and 10). Transparency is a precondition for sustainable supply chain management. Certain critical technologies such as blockchain (see our comment on "Critical Technologies") promise to increase the transparency about the origins of natural resources and other goods.

[1] ASIC (2021): Cyber resilience of firms in Australia's financial market: 2020-21, Report 716, December 2021, available at: https://download.asic.gov.au/media/fmfdhegw/rep716-published-6-december-2021.pdf (accessed 18 January 2022).

Recommendation 3:

Traceability be added to the transparency principles.

In our view, *Principle 5*, should receive stronger emphasis. ”Know your supplier” should help businesses safeguard against security risks and support them embrace more sustainable, environmentally- and human rights-focused processes (see our comments on Principles 9 and 10). “Know your supplier” provisions could include minimum transparency principles consistent with existing standards and international benchmarks’ as proposed in *Principle 6*.

We support *Principle 6*. Minimum transparency principles should reduce the susceptibility and vulnerability of supply chains and increase supply chain resilience. SMEs will require support to understand what comprises these ‘existing standards and international benchmarks’ for transparency.

Recommendation 4:

A list of existing standards and international benchmarks for suppliers be published and/or template examples of minimum transparency requirements for supply contracts be provided.

While we support *Principle 7*, the challenging nature of monitoring and assessing an entire supply chain should be recognised, especially for SMEs. Businesses will need guidance on how to meet *Principle 7*.

Autonomy and integrity

We question businesses’ capabilities to adopt *Principle 8*, especially SMEs Unless the federal government supports businesses in understanding and being able to consider the level of foreign government influence, it is very difficult for businesses to make such assessments. The federal government is best placed to share intelligence with business on the influence foreign governments have on suppliers.

While “consider if” suppliers operate ethically, with integrity and in alignment with human rights as proposed in *Principle 9* is currently sufficient, it may not be in the future. Businesses should be encouraged to conduct appropriate due diligence of their supply chains.

Several other jurisdictions are currently either discussing, developing, or mandating sustainability and ESG principles for supply chain management. We don’t expect this trend to fade. For example, the 2021 German Act on Corporate Due Diligence in Supply Chains imposes, for the first time, a binding obligation on companies to establish, implement and update due diligence procedures to improve compliance with specified core human rights and, to a limited extent, environmental protection in supply chains. It will see German companies held legally responsible for any human rights or environmental abuses found across their global supply chains. This law will not only apply to companies with their registered office in Germany, but also to foreign companies that have a branch office in Germany.[2]

This law could be a blueprint for a uniform European regulation on supply chain sustainability. We expect similar regulatory developments across the world and encourage the federal government to consider these developments in any future action it may take on supply chain sustainability.

Australia has adopted the Modern Slavery Act 2018, that “requires (sic) some entities to report on the risks of modern slavery in their operations **and supply chains** (emphasis added) and actions to address those risks, and for related purposes”. We note that this Act limits mandatory compliance to those entities with a consolidated revenue of at least $100 million (5)(1)(a), but does make provision for voluntary adoption (5)(1)(d).

The government should provide information on what “consistently with international law and human rights” implies. We suggest that any guidance be in line with the UN Sustainable Development Goals (SDGs), UN Guiding Principles for Business and Human Rights and international labor and worker conventions where applicable.

[2] The Act will come into force on 1 January 2023, giving companies a transitional period to prepare for their new supply chain due diligence obligations by revising their existing compliance management systems, establishing new processes, and training their employees accordingly.

We therefore advocate for the inclusion of “sustainability” in *Principle 9*.

Recommendation 5:

Principle 9 be amended to “Consider if suppliers operate ethically, *sustainably*, with integrity, and consistently with international law and human rights.”

Considering the several supply chain threats mentioned earlier, especially being over-reliant on one supplier or suppliers from a similar geographic area, we suggest *Principle 10* be expanded.

Recommendation 6:

Principle 10 be amended to “Build strategic partnering relationships with critical suppliers *and avoid over-reliance on single suppliers.”*

Critical and Emerging Technologies

We note that the Principles must be technology-neutral to remain relevant for emerging and new technologies.

Adding to the technologies mentioned in the consultation paper (e.g., artificial intelligence and quantum computing), we note that Australia’s Digital Economy Strategy 2030 lists further critical technologies and/or solutions with the potential to improve supply chain resilience:

- using **big data** and **advanced data analytics** to analyse risk exposure and identify potential shortages of critical supplies
- introducing **labelling** standards to improve integration of digital supply chain systems and decrease operating costs
- using digital solutions, such as digital control towers or **blockchain**, to improve transparency of supply chains and inventories

Although the outcome of government’s blockchain pilots have not yet been released, we note blockchain technology’s potential impact on supply chains has received significant attention. Blockchain’s features bear relevance for all Principles. We emphasise its ability to enhance transparency and traceability. By tracking individual products from the point of production to the end consumer, blockchain could further enhance sustainability.

We encourage the government to further support technology pilots relevant to enhancing supply chain resilience and supply chain agility.

Recommendation 7:

The Government extend its support of further technology pilots focused on improving supply chain security, transparency and traceability as well as sustainability.

In considering supply chains of the future, we expect greater levels of automation and note that other jurisdictions (e.g., Singapore) already support end-to-end data platforms that enhance consistency and real-time data visibility, offer greater security along supply chains and help to identify and manage supply chain risks.

Critical technology supply chains involving several different parties and using a vast range of digital solutions, must be interoperable to avoid disruptions. Digital interoperability concerning data or information exchange becomes a key enabler for the supply chains of the future.

Recommendation 8:

Government to consider digital platforms and technology interoperability to improve supply chain resilience and agility.

Our recommendation reflects the Australian government’s National Freight and Supply Chain Strategy, which – amongst others – encourages the adoption of collaborative electronic platforms along supply chains by 2024.

Government's role

Recognising that the pandemic has amplified the need to digitally transform, it's important that the government continues incentivising and encouraging businesses to accelerate the rate of digitalisation at the enterprise level and uplift digital competencies of supply chain participants.

We note that Australia's Digital Economy Strategy 2030 emphasises the need for large businesses to support the digitalisation of SMEs in their supply chains. Whilst we were not able to identify relevant collaborations between large businesses and their smaller counterparts in Australia, we understand that in Singapore the Alliance for Action (AfA) on Supply Chain Digitalisation held workshops that brought together large multinationals, SMEs, startups, and government agencies. In a collaborative manner, all participants identified pain points and opportunities across the supply chain. Through these workshops, the AfA arrived at a solution of a common data infrastructure (CDI) to enhance interoperability between supply chain platforms and provide all stakeholder groups, including SMEs, with better access to those platforms.

Introducing similar government-led initiatives in Australia would potentially offer opportunities for SMEs, such as enabling access to new markets by onboarding SMEs to large businesses' digital supply chain platforms/solutions.

Recommendation 9:

The Federal Government launch an initiative to bring together businesses across all sizes to identify supply chain pain points, develop solutions and collaborate.

Connecting SMEs to technology supply chain opportunities is essential to increase SMEs' access to cross-border e-marketplaces and financing, and to help SMEs enhance digital adoption.

As part of this initiative, the government should continue to focus on reskilling and upskilling workers and SME owners. Digital skills and competencies such as platforming, data analytics and visualisation, and supply chain modelling and planning are crucial.

Recommendation 10:

Funding for the upskilling and reskilling efforts be significantly increased so that small businesses and workers keep pace with Australia's transition to a digital economy.