CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

SUBMISSION:

Critical Technology Supply Chain Principles – Discussion Paper

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: Critical Technology Supply Chain Principles – Discussion Paper

I am pleased to make this submission to the Department of Home Affairs on behalf of the Cyber Security Cooperative Research Centre (CSCRC) regarding the draft *Critical Technology Supply Chain Principles* (the Principles). The CSCRC commends the Federal Government for its ongoing commitment to ensuring Australia remains a safe and prosperous nation and an exemplar, globally, at securing future-focused and emerging technologies essential to Australia's national and economic security.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

The CSCRC is a public company limited by guarantee and will invest $AU50 million of Australian Commonwealth Government funding and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas. The CSCRC has 25 Participants including seven Research Providers, eight State and Federal Government Agencies/Departments and ten Industry/SMEs.

We look forward to answering any queries regarding this submission and welcome the opportunity to participate in future discussions on this very important topic.

Yours sincerely,

Rachael Falk, CEO, CSCRC
ceo@cybersecuritycrc.org.au

Executive Summary

The Cyber Security Cooperative Research Centre (CSCRC) welcomes the opportunity to provide this submission to the Department of Home Affairs in response to the publication of its draft *Critical Technology Supply Chain Principles – Discussion Paper*, regarding opportunities to secure and ensure the integrity of Australia's critical technologies and mitigate against supply chain risks. This discussion paper is particularly timely given the pronounced impact rising geostrategic competition during the COVID-19 pandemic continues to have on global supply chains and the technological developments that underpin them, which are increasingly embedded and integrated into the fabric of everyday life.

In recent years, strategic competition for global technological pre-eminence has accelerated. Concurrently, the global supply chain has been re-ordered, with China overtaking the United States in 2010 as the world's top manufacturer[1], leading to concerns about the West's over-reliance on Chinese-led supply chains and China's subsequent growing influence on the global technological order. In recognition of the potential ability for technology to shape future normative values, systems and economic, geopolitical and political outcomes, Australia's allies and partners around the world have signalled their intent to secure future-focused capabilities. On that front, the United States recently published a *National Strategy for Critical and Emerging Technologies*[2], which establishes critical areas where the United States seeks to maintain competitive advantage together with its key allies, presenting a list of 20 technologies deemed critical to the national security of the United States.

Australia is also working to shore up the adoption of critical technologies. This discussion paper signals the increasing significance of this issue to Australia's future economic and national security. To that end, the CSCRC welcomes the Federal Government's concerted efforts to maintain the autonomy, security and transparency of Australian supply chains and ensure our nation's economy is ready to meet the challenges of a post-COVID-19 world.

[1] https://www.reuters.com/article/us-health-coronavirus-usa-china/trump-administration-pushing-to-rip-global-supply-chains-from-china-officials-idUSKBN22G0BZ
[2] https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf

Key recommendations

- The Federal Government should take steps to make the Principles mandatory through the establishment of clear standards and regulatory frameworks.
- The business community must be proactive in supporting the Principles and uplift in the security of critical technology supply chains, which would be assisted by the establishment of clear baseline standards and regulatory frameworks.
- The Principles should be subject to annual review, which will help ensure they remain fit-for-purpose in what is a quickly evolving space.
- The Federal Government should define what constitutes a critical technology and what is to be prioritised. It is suggested that the starting point must be defining what is, and what is not, critical technology.
- Mandatory minimum standards must be established to effectively secure critical technology supply chains.
- The voluntary *Code of Practice: Securing the Internet of Things for Consumers* should become mandatory, using a phased-in approach, which would encourage greater implementation of secure-by-design principles.
- The reporting threshold of the *Modern Slavery Act 2018* should be lowered to capture businesses and entities with a consolidated revenue of $50m.
- An incentivisation program should be established to encourage business uptake of the Principles, which could include measures such as tax breaks and instant asset write offs.
- The Federal Government should implement the Principles across its functions and make procurement decisions that support sovereign critical technology capabilities.
- Within the Security-by Design Principles there should be an additional Principle, which focuses on research and development to enhance security-by-design.

1. Do you think there is a need for Government to address the security of critical technology supply chains?

The CSCRC strongly believes that shoring up the security of critical technology supply chains is essential to ensuring Australia's future prosperity and reputation as a safe and trusted place to do business. Government has a key role to play in this process, with the designated authority to mandate standards and apply regulatory frameworks that set clear guidelines and principles for business to operate within. That said, ultimately there is little point in promoting the security of critical technology supply chains without regulatory frameworks to support such a shift. There are strong indications from the business community that clear frameworks are a help, not a hindrance, especially given the regulatory complexity that companies must navigate, both now and in the future.

While the responsibility for mandating clear standards and regulatory frameworks is the remit of government, the business community must also be active participants in and proactive supporters of an uplift in the security of critical technology supply chains. As noted above, this will be assisted by the establishment of clear baseline standards and regulatory frameworks. Anecdotally, when speaking with business, the CSCRC notes there is an appetite for uplift but this is an area in which clear and ongoing guidance and support is required. Hence, close and early consultation with industry must be a key component when addressing the security of critical technology supply chains, with broad consultation required to ensure that any changes are industry-driven and not a handbrake on market gains.

Furthermore, the COVID-19 pandemic has highlighted the threats to and potential fragility of global critical technology supply chains. Amid heightened geopolitical tension between powerful nation states, there is a parallel effort to move away from the primacy of existing overseas supply chains[3] to secure sovereign products and services and to decouple, technologically, from nations that may pose a threat to national sovereignty. In Australia, there is a marked need for domestic capacity and capability and the implementation of secure-by-design principles into supply chain management and critical technologies. Research undertaken by the CSCRC and CSIRO's Data61 on consumer attitudes to the cyber security of IoT devices clearly illustrated there is demand for built-in and effective cyber security features and support for a cyber security rating system, which 75 per cent of survey respondents indicated would influence their purchasing decisions[4]. While such an example does not directly relate to security of critical technology supply chains it does support anecdotal evidence that across the entire ecosystem there is a need and demand for cyber security uplift.

[3] https://thediplomat.com/2020/07/covid-19-complicates-the-us-china-cyber-threat-landscape/
[4] Report: Internet of Things (IoT) Consumer Research, CSCRC and CSIRO's Data61, 2020

2. How do you think the suggested Principles will help address the need for trusted critical technology supply chains? Does anything else need to be adjusted or included?

The CSCRC notes the suggested Principles will help address the need and support the development of trusted critical technology supply chains because fundamentally they highlight the key issues businesses must consider – the Who? What? How? When? Where? and Why? While such an analysis may appear elementary, it is the correct approach to take, as it helps break down what is a complex and technical area into smaller, easier to address segments. In the event of disruption, having answers to these questions will also assist businesses and government in ensuring appropriate and secure workarounds can be established in a timely and effective manner.

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 2018*[5] (the Act) provisions. The Act encourages businesses to take a technology-led approach to monitoring supply chains, providing rigorous and largely incorruptible visibility into these supply chains. This not only assists organisations to ensure exploited workers are not being used to produce goods and services feeding into their supply chains, it also helps assure the origins of these goods and services do not present a national security risk. These considerations are increasingly important given heightened international scrutiny of products and goods manufactured under potentially exploitative conditions. For example, it is worthwhile to note the Australian Strategic Policy Institute's (ASPI) recent *Uyghurs for Sale*[6] report, which exposes the exploitation of Uyghurs in Chinese 're-education' camps. The report found that a range of large multinationals, including global technology companies that have a significant market presence in Australia, were using components in their products that were likely produced using Uyghur labour. To that end, the CSCRC commends the concerted effort currently underway by various stakeholders to bring visibility and transparency to these issues and to ensure the integrity of global supply chains from a human capital perspective.

While the Principles are sufficiently broad to cover current issues and concerns, the CSCRC recommends they be subject to regular (annual) review, which will help ensure they remain fit-for-purpose given the rapidly evolving cyber security threat landscape. The rapid proliferation of new technologies and their ability to outpace the regulatory frameworks within which they operate remains problematic. Regular review would help mitigate risks that could arise from legislative 'lag' by ensuring issues are dealt with in a timely matter and regulation is not constantly playing catch up.

Critically, the CSCRC recommends that specific guidance be forthcoming from government as to what constitutes a critical technology in the Australian context. As previously noted, in the United

[5] https://www.legislation.gov.au/Details/C2018A00153
[6] https://www.aspi.org.au/report/uyghurs-sale

States' *National Strategy for Critical and Emerging Technologies* (the Strategy), a list of 20 technologies categorised as critical, or potentially critical, to the US' national security advantage were identified. The Strategy advocates a holistic, comprehensive approach to these technologies and the potential for possible technological convergence across them. The list, which will be reviewed annually, includes: advanced computing; advanced manufacturing; artificial intelligence; autonomous systems; data science and storage and quantum information science, among others. Furthermore, the Strategy presents preliminary measures to achieving success in this domain.

The lack of clear guidance as to what the Australian government considers to be a 'critical technology' is problematic. Only once definitional clarity has been achieved can there be conceptual clarity for stakeholders. The CSCRC submits that early consideration be given as to what technologies are to be prioritised by government with such definitional clarity provided sooner rather than later. Furthermore, any definition or list of technologies should be subject to annual review, given the fast-moving pace of technological development. Given Australia's longstanding relationship with the United States as a key ally and partner, it makes sense the government might consider drawing from its approach in the interests of alignment, global interoperability and harmonisation of regulatory frameworks.

5. What additional advice, guidance or tools would you require from Government to effectively apply the suggested Principles?

While it is admirable the government is tackling this important issue by taking a principles-based approach, the CSCRC submits that over time, to achieve the uplift that is required, mandatory minimum standards must be established to effectively secure critical technology supply chains. Given the government is moving towards mandated minimum cyber security standards for various sectors through signposted changes to the *Security of Critical Infrastructure Act 2018*, it would make sense for critical supply chain standards to be applied concurrently, through a phased approach[7], modelled after the General Data Protection Regulation (GDPR) model. This would in turn, encourage the implementation of secure-by-design principles during critical infrastructure uplift, assist in achieving economy-wide harmonisation and serve to mitigate piecemeal integration. While there is no doubt such an undertaking would be onerous on businesses and government, it would have the effect of setting clear and holistic parameters which, as previously noted, is the desire of business.

[7] https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000

The Federal Government's release of the voluntary *Code of Practice: Securing the Internet of Things for Consumers*[8], is a positive first step to increase the cyber security of IoT devices in Australia. However, given the Code is voluntary and therefore unenforceable, it is very limited in what it can materially achieve. Moving forward, the CSCRC submits that the Code should become mandatory, using a phased-in approach. This would help ensure that at the most basic level, secure-by-design principles are integrated into the majority of IoT devices in the Australian market, resulting in cyber security uplift across the entire ecosystem. This would ultimately help harden critical technology supply chains and ultimately contribute to a consumer cyber security uplift. Such a code would be well supported by an IoT device rating system. As noted earlier, CSCRC research indicates there is consumer demand for such a rating system, which would also have significant advantages for business too. This includes Australian tech businesses that produce IoT and cyber security devices and services, encouraging uplift at the design stage and presenting an opportunity to leverage market uptake as a result.

As previously noted, the security of critical technology supply chains will be both supported and bolstered by the provisions of the *Modern Slavery Act 2018*[9]. However, in its current form the Act only applies to large businesses and entities in the Australian market with a consolidated revenue of at least $100m. These businesses are required to prepare annual modern slavery statements, which identify and mitigate modern slavery risks in their global operations and supply chains. The CSCRC submits that this threshold should be lowered to capture businesses and entities with a consolidated revenue of $50m. Such a move would capture a broader cross-section of Australian businesses or global entities operating within Australia and, as a result, more threats to critical technology supply chains could be detected.

8. What could Government do to increase the uptake of the suggested Principles? What else do you think Government could consider to help make the supply chains of critical technologies more trusted and resilient?

The CSRC submits there are two key steps the government could take to increase uptake of the Principles. First, as previously noted, while the Principles are being introduced as voluntary guidelines, steps should be taken over time to make them mandatory. In doing so, a clear framework within which business can effectively operate with certainty will be established. Second, there is no doubt that implementing the Principles will come at a cost to business. Hence, the CSCRC suggests various incentivisation schemes should be considered for businesses that can illustrate they have

[8] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice
[9] https://www.legislation.gov.au/Details/C2018A00153

applied the Principles. Such measures could include tax breaks and instant asset write-offs. This would have a two-pronged effect and make economic sense, encouraging business to implement the Principles while also hardening Australia's critical technology supply chains, reducing the likelihood of disruption and associated negative economic impacts in the future.

The CSCRC contends that government also has a key role to play by implementing the Principles across its functions and making procurement decisions that support sovereign critical technology capabilities. In this area, government must be seen to be leading by example. Steps must be taken to ensure innovative leading technologies developed in Australia by Australian entities are leveraged domestically and, especially in their infancy, are procured by government where appropriate to build capacity and scale. This would have a trickle-down effect and help ensure that domestically produced technologies are taken up more broadly. Importantly, it would also ensure domestic producers of critical technology can operate on an even playing field with more established foreign entities, building Australia's sovereign critical technology supply chain capacity moving forward.

Finally, as previously noted, the government should take steps to make mandatory the voluntary *Code of Practice: Securing the Internet of Things for Consumers*[10]. Such a move would be well served by the establishment of a robust domestic IoT device rating system.

9. Is there anything else the Government should consider when finalising the proposed Principles?

While the Principles are currently fit-for-purpose, they should be subject to annual review to ensure they remain relevant and up to date in what is a rapidly evolving technology environment. As we have seen in Australia – and has also been the experience of other developed states – regulation has generally failed to keep pace with technological advances. Implementation of the Principles presents a clear opportunity for the Federal Government, through regular review, to ensure the provisions outlined remain fit-for-purpose.

One thing the Principles lack is mention of the central role research and development will play in protecting critical technology supply chains. The CSCRC submits that within the Security-by Design Principles there should be an additional Principle, which focuses on research and development to enhance security-by-design. For example: *"Invest in research and development to help ensure security provisions evolve in line with current and emerging threats"*.

[10] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice

Finally, as previously noted, an incentivisation scheme should be considered for businesses that can illustrate they have applied the Principles, which could incorporate measures like tax breaks and instant asset write offs.