Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

11 November 2020

Dear Sir/Madam,

AIIA Submission to the Critical Technology Supply Chain Principles: A call for views.

Thank you for the opportunity to make a submission in respect of the proposed Critical Technology Supply Chain principles.

About the AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. We are a not-for-profit industry association and since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity.

We do this by delivering outstanding member value by:
• providing a strong voice of influence;
• building a sense of community through events and education;
• enabling a network for collaboration and inspiration; and
• developing compelling tech policy thought leadership, government submissions and supporting state and federal government roundtables, committees and reviews.

We represent a large and diverse number of technology organisations in Australia, including:
• Multinational companies including all the major cloud platform providers and software vendors;
• National organisations including data centre owners, cloud providers, telecommunications companies and other tech leaders; and
• a diverse and large number of small and medium businesses, start-ups, universities and digital incubators.

Introduction

The AIIA supports government leadership in ensuring the digital economy is secure and resilient. Better informed businesses, industries sectors, governments and individuals as to cyber risks and supply chain vulnerabilities are important considerations for a modern digital economy. The AIIA is aware of the dual process the Department of Home Affairs is running concerning regulating an increased list of Critical Industries across many sectors of the economy in response to cybersecurity threats. We believe that government should have a coordinated approach to dealing with these reviews, in an orderly and stepped fashion, rather than having multiple processes underway simultaneously.

The latest ACSC Annual Cyber Threat Report[1] covering July 2019 to June 2020 reported that it responded to 2,266 cyber security incidents and received 59,806 cybercrime reports at an average of 164 cybercrime reports per day, or one report every 10 minutes. As the report makes clear, phishing and spearphishing are the most common threats that can lead to ransomware attacks. A key weakness in Australian business' cyber security is that of human weakness by clicking on unsolicited emails and links. Awareness campaigns may be one area of government consideration.

A second area of concern the ACSC reports is the growing 5G network and use of IoT devices. In our white paper[2], we discuss these vulnerabilities, reference the transport and freight sectors as an area of potential weakness in our supply chains, not just from a technology point of view but for disrupting the distribution of vital goods around the country. The ACSC report also says:

> "*Australians need to be mindful that cyber adversaries are constantly looking for vulnerabilities and weaknesses in systems and networks. The ACSC continues to identify many products and services being adopted and implemented by organisations that lack 'secure by design' principles.*
>
> *Applying the fundamentals of good cyber security as individuals, business owners and government agencies is vitally important and in many ways Australians are not necessarily learning from past experience. The ACSC responds to hundreds of cyber security incidents each year. Many of these could have been avoided or substantially mitigated by good cyber security practices.*
>
> *Implementing ASD's Essential Eight[3] security controls will substantially reduce the risk of compromise, and help to prevent the most common tactics, techniques and procedures (TTPs) used by malicious cyber adversaries". (p4).*

Cyber resilience and cybersecurity

It is also important that when considering supply chain vulnerabilities for critical technologies that the distinction between cyber security and cyber resilience is well understood and as the lead sentence of the government paper says: "*Supply chains for critical technologies in Australia must be more **resilient**"* (emphasis added).

[1] https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf
[2] https://aiia.com.au/__data/assets/pdf_file/0017/103562/Building-Australias-Digital-Future-in-a-Post-COVID-World-AIIA-Whitepaper-2020.pdf
[3] https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-explained

Cybersecurity and cyber resilience are distinct concerns and understanding the difference by industry is key to preparing an effective response to cyber threats. The misconception that a cybersecurity program can substitute for cyber resilience is potentially disastrous. While cybersecurity focuses on keeping attackers out, cyber resilience aims instead to minimize the mayhem caused by attackers who do manage to penetrate networks.

As cyber threats evolve, some are suggesting that cybersecurity ratings are poised to become as important a factor as credit ratings, making failure to implement a professional cyber resilience program more than a reputational risk. A thoughtfully designed cyber resilience program will become not only a competitive advantage but a requirement for sustained growth.

The government could give consideration to developing ratings of critical supply chain technologies that would provide useful guidance for industry, individuals and business. This guidance would be based on adherence to trusted and known existing standards and leverage existing Australian government assurance frameworks like the IRAP.
MIT and Sloan suggest that there should be four-phases to a cyber resilience framework — preparation, detection, response, and recovery — that can enhance an organization's capacity to sustain operations through a cyberattack while minimizing both disruption and reputational harm.

Advice in extreme circumstances

The Government should consider the mechanisms that are available to it to issue directives and advice to public and private sectors on supply chain risks in the event of extreme circumstances. The Australian Cyber Security Centre (ACSC) issues alerts in relation to at-risk products and other cybersecurity threats on its website, but for higher-level cyber threats that might have a broader impact on business and the economy, it may consider best-practice mechanisms for broader notification and risk-mitigation. [4]

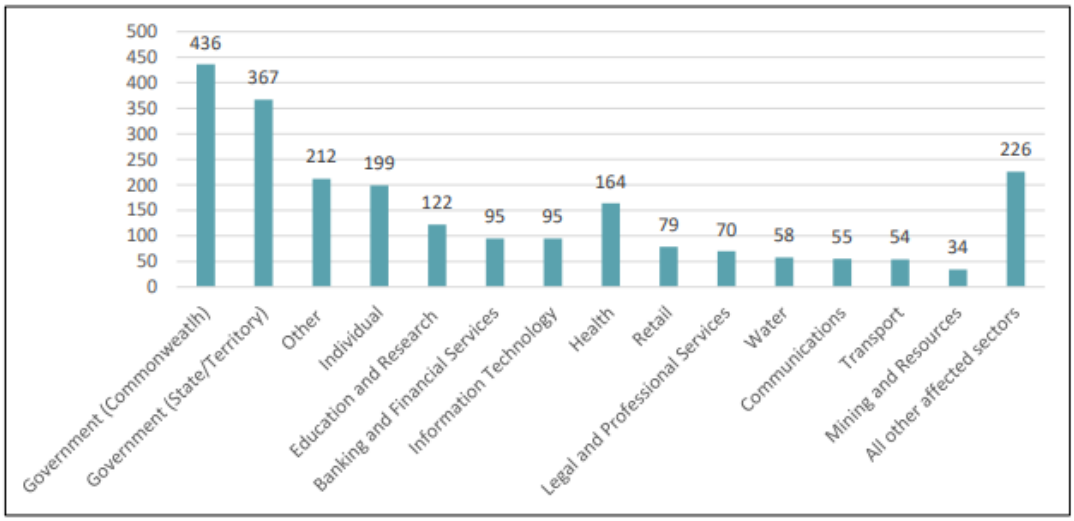
Critical Industries: already an expanded requirement by government to report and protect supply chains

The proposed principles could be reviewed and updated once the critical industries sectoral regulations and standards and adopted. It would seem a sensible place for the government to start that the increased awareness and capability of cyber threats focus on those industries previously having been identified by the government, namely:

- Banking and finance
- Communications
- Data and the Cloud
- Defence industry
- Education, research and innovation
- Energy
- Food and grocery
- Health
- Space
- Transport
- Water

[4] As an example, approximately two years ago, the United States Department of Homeland Security, in consultation with interagency partners, determined that the risks presented by Kaspersky-branded products justify issuance of a binding operational directive to remove and discontinue present and future use of all Kaspersky-branded products within 60 days.

Figure 3: Cyber security incidents, by affected sector (1 July 2019 to 30 June 2020)



As shown in Figure 3, a large proportion of incidents are reported by Commonwealth, state and territory governments (35.4%, n=803). The comparatively higher volume of reports from Commonwealth, State and Territory Governments is due to their close working relationship with the ACSC and their willingness to report incidents. Australia's critical infrastructure sectors including electricity, water, health, communications and education represented around 35% of the incidents responded to by the ACSC. [5]

The 10 principles and three pillars of critical technology supply chains

The AIIA supports the three pillars of security-by-design (along with privacy by design), transparency and autonomy and integrity. Noting that supplier code of ethics and transparency around human rights and human slavery for example have been adopted by many Australian businesses already.

Further, the AIIA supports the consideration of existing standards, be they international or local, as a way to ensure supply chains meet minimum cyber security requirements. This is referenced under Transparency in Pillar 6. The AIIA would be concerned if, through this Critical Technology Supply Chains process, additional standards be developed or recommended, noting that there is a parallel process underway by the Department of Home Affairs regarding regulated Critical Industries.

Pillar 8, however, has the potential to cause some confusion and the AIIA would argue does not provide guidance and clarity for readers of the Principles:

> *Consider the influence of foreign governments on suppliers and seek to ensure they operate with appropriate levels of autonomy*

The ability for some companies where technology is not a core capability and maturity levels not well developed such as many SMEs in our economy, may find it difficult to interpret Principle 8 around which are "good foreign governments" and those critical technologies within that country pose more "risk" than other countries and technologies.

[5] Source: Australian Cyber Security Centre, 'Annual Cyber Threat Report July 2019 – June 2020', cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf, p.7

Governments should play a positive role in supply chain risk management, avoiding using simplistic factors such as the country of origin of a service or product to assess risk. Information sharing from the Government would be more helpful versus making the private sector guess how aligned foreign governments are with Australian laws and national security goals.

The paper on page 12 makes the issue potentially more unclear in that it seems to place any large technology company as a risk which we assume is unintended and could also affect a number of successful Australian companies operating in a number of markets and makes it harder for the Australian public to understand the real intent:

> *If you use a supplier that operates in multiple countries with differing laws, you (the consumer or end-user) should take into account potential risks to your supply chain, even when that organisation does not disclose a direct conflict.*

The AIIA believes that the government may wish to re-consider how this principle can be applied and interpreted by the ”average” business so that it is clear and in fact whether this is the best mechanism at the government’s disposal to reduce the use of technology that could be directed for misuse by a foreign power. This issue may be better dealt with either through an outright bans of the technology, as has occurred in the 5G infrastructure space, or in the critical industries regulations and standards, other international and national standards or the suggested ratings system.

Industry Engagement Mechanisms, Incentives and Case Studies

The AIIA would consider it desirable for the Government to establish forums or other mechanisms for engagement with industry regarding supply chain risk management, both in terms of what the standards should ‘look like’ – and continue to look like – but also to co-develop guidance and provide support for industry to understand how to implement these high-level principles. The AIIA would welcome an opportunity to liaise with government to co-design further principles and standards. This could include an identification of supply chain risks and guidance as to how to mitigate them in practice as well as creating incentives for companies to adopt best practices in supply chain risk management, as well as consider sharing some case studies of companies that demonstrate good supply chain practices to assist industry to realise how key principles have been successfully applied.

Conclusion

A final note of caution in regard to framing principles around global supply chain risk is that it must be recognised that Australia does not have an advanced manufacturing capability of technology such as silicon chips, phones, computers and laptops.Diversifying away from specific international markets for certain products may prove extremely difficult and in fact is not a concern in most cases with no local capability being considered nor likely to be created. It is important to underline that Australia’s future economic prosperity continues to be tied to open global markets and exports and the AIIA fully supports Australian and international efforts to ensure transparent, non-discriminatory trade.

Yours sincerely,

Simon Bush
GM Policy and Advocacy, AIIA