Australian Government

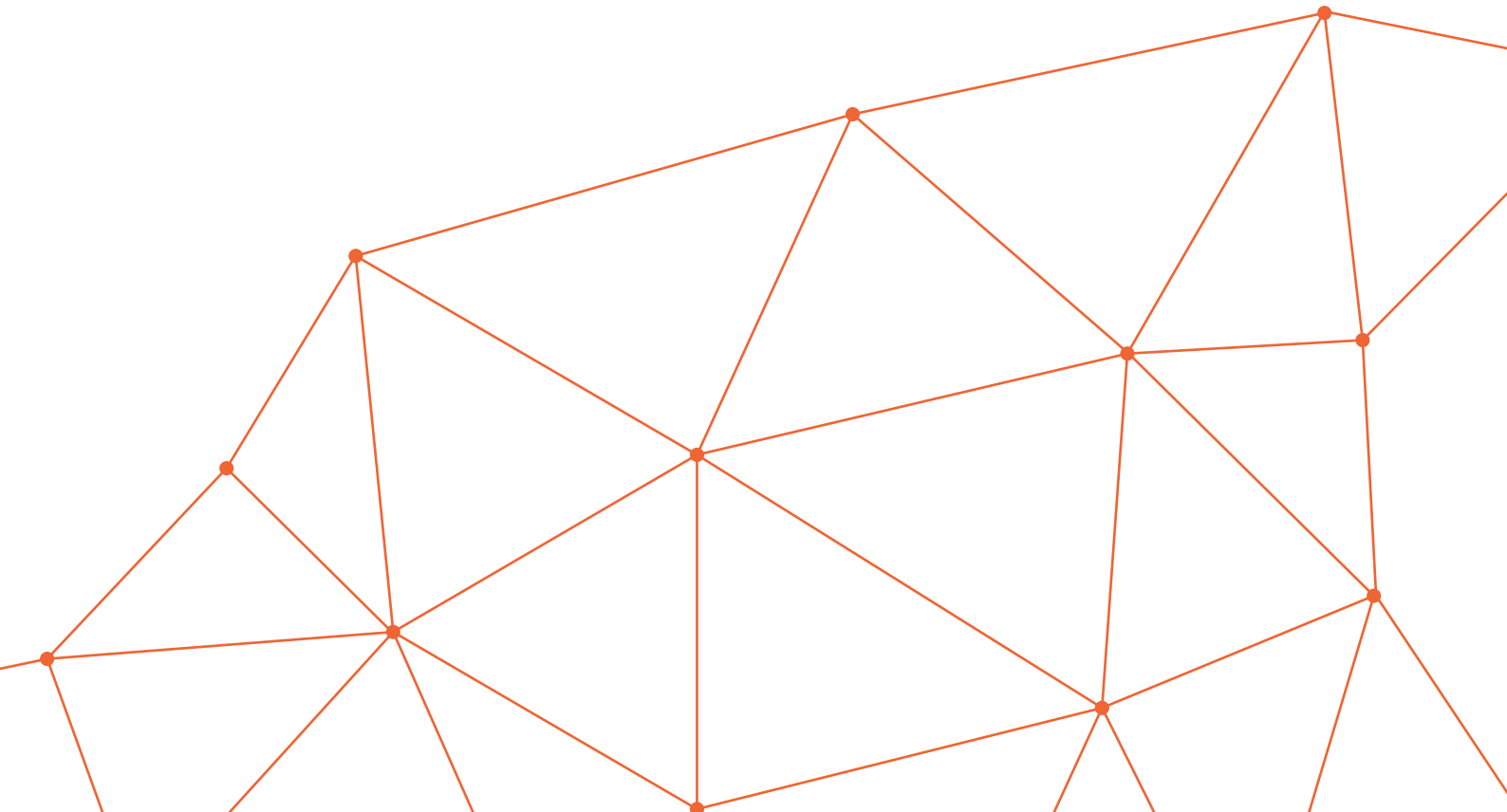
Critical Technology Supply Chain Principles

Summary of public consultation

Contact us

Enquiries regarding the licence and any use of this document are welcome at critical.technology@homeaffairs.gov.au.

Contents



Introduction

The Critical Technology Supply Chain Principles (the Principles) are designed to improve the resilience of supply chains for critical technologies in Australia. Improving the management of critical technology supply chains across the economy will help build Australia's resilience to future shocks, as well as help to address the inherent risks to our nation's national security, economic prosperity and social cohesion.

The Department of Home Affairs (Home Affairs), along with the Department of Industry, Science, Energy and Resources (DISER), has developed the Principles through a co-design process with industry participants. The co-design process has served to ensure the Principles are fit for purpose, benefit those who adopt them and are easy to apply so organisations can securely adopt critical technologies.

This consultation follows and complements the public engagement on *Australia's Cyber Security Strategy 2020* and reforms to protect *Critical Infrastructure and Systems of National Significance*.

A public discussion paper was released on 22 October 2020 to start the co-design process. The discussion paper posed a range of questions and invited views on the draft Principles that were developed by a range of Government experts. Written submissions were invited for a two-week period. Submissions, received over a two week period, came from companies of all sizes, non-government organisations, state and territory governments, and members of the community.

Following this period, the Government hosted a number of workshops with a variety of targeted industry participants to build on initial engagement. During the workshops, participants reviewed, tested and refined the draft Principles to ensure a range of views were captured and reflected in the Principles.

Feedback asked that consideration be given to the fact that the development of technology, especially critical technology, is the result of many years of investment and development. Some forms of technology are derived from limited resources and the replication or replacement of them would require significant resources and time[1], which could have a disproportionate impact on small to medium enterprises relative to large businesses.

The final workshop with industry participants focused on implementation and evaluation of the Principles. While the Principles are voluntary for industry there was significant support for the final Principles and the way they will support the security of critical technologies. The consultation highlighted that it would be useful for Government to provide additional documentation as the Principles are implemented, and provide clear guidance and supporting material on how organisations could implement the Principles.

The Australian Government appreciated all of the feedback on the Principles and the time taken to engage with this process. Conversations and written feedback covered a range of topics across this complex issue, and the Government appreciates the expertise and insights that were provided on how best to secure critical technology supply chains.

The Principles will be used as part of the Australian Government's decision making processes, and will conduct a review after 12 months. We welcome any party to apply the Principles over this period and provide feedback to critical.technology@homeaffairs.gov.au. This feedback will then be used to develop case studies and help build further guidance material.

1 *Confidential Submission 13*

General Feedback

Overall, feedback was supportive of the Principles through the consultation process. Industry feedback agreed that critical technology supply chain security is increasingly important to ensure Australia's future economic prosperity and national security.[2] Responses flagged that government and industry partnerships are key in ensuring that industry has the full threat picture.[3]

We heard that most businesses are aware of the risks to their critical technology supply chains, however they require clear definitions from Government on what constitutes a critical technology, and what should be prioritised[4]. There was also discussion around whether the Principles, which are currently voluntary, should be mandatory or not. Some businesses supported mandatory Principles, through the establishment of clear standards and regulatory frameworks[5] with Government support[6]. We heard that mandating the Principles could be considered at their 12 month review.[7]

We also heard that making the Principles mandatory could erode their usefulness to industry and limit flexibility. If the Principles were to become mandatory, there should be evidence to support their measurements of success and a framework to report compliance[8]. There was strong support for Government to implement the Principles first, and provide case studies to industry outlining the costs, benefits and risks[9]. We will continue this conversation with industry partners through the evaluation and implementation process for the Principles.

It was repeated throughout the consultation process that Government could provide more in-depth guidance under each principle to support their implementation. Industry partners advised that Government could provide pragmatic questions entities can ask of themselves and their suppliers as they work toward supply chain resilience.[10] Feedback highlighted that best practice guides could support adaptation of the Principles. Responses highlighted that awareness raising and education on supply chain security is required[11]. Additionally, it was noted that successful case studies and evidence of the Principles effectiveness would empower industry uptake.

There was feedback from multiple respondents that the Principles coincide with the objectives of existing standards – specifically the Australian Signal Directorate's *Information Security Manual* and Department of Home Affairs' *Telecommunications Sector Security Reforms.*[12] We also heard that it is important that the Principles recognise the other various initiatives in place or underway to ensure any crossover is considered.

We heard the feedback that the Principles have the ability to shape decisions of companies of all sizes. The Principles can provide a baseline for companies that are scaling and might require initial guidance on supply chain management. They may also be of use to entities across the public or private sector who wish to assess their supply chain resilience and security posture.[13]

2 *Cyber Security CRC*
3 *Telstra Cooperation Limited*
4 *Cyber Security CRC*
5 *Cyber Security CRC, Confidential Submission 18, Sapien Cyber, Cisco Systems Australia Pty Ltd*
6 *Oceania Cyber Security Centre, Sapien Cyber, Cisco Systems Australia Pty Ltd*
7 *Confidential Submission 18*
8 *The Software Alliance (BSA)*
9 *Advisory Board Centre, Sapien Cyber*
10 *Confidential Submission 20*
11 *SoftIron, Advisory Board Centre*
12 *Telstra Cooperation Limited*
13 *Standards Australia*

Through submissions and discussion with industry participants, implementation considerations were also raised. This included the suggestion that to encourage compliance there could be reporting requirements for organisations and major products, similar to reporting requirements in modern slavery reporting. This could involve organisations confirming that they had considered the principles in their operations. Government could consider mechanisms to be able to measure progress by businesses and Government entities. This could be done through voluntary, targeted surveys, via a self-reporting framework or other data gathering mechanisms that do not significantly add to administration costs.[14]

Additionally, respondents noted that the cheapest option is not always best when it comes to security. Costs are difficult to estimate, however from a risk management perspective, the costs of not addressing supply chain risks are far greater. Government should ideally enable sensible financial decisions by empowering staff to consider, with prudent weight scales, other values alongside lowest cost models.[15] Implementing mandatory principles would likely impose administrative costs, but costs could likely be offset by the benefit of a more security-ordinated culture outside of Government and a greater focus on supply chain resilience.[16]

Finally, it was clear that Government and industry must collaborate to ensure that the security of critical technology supply chains is well-informed, robust and continually adapting. The evolving pace of innovation at the national level, and international level, is underpinned by the competitive element nature of the market and requires cooperation to ensure the Principles can be actively applied.[17]

14 *Cisco Systems Australia Pty Ltd*
15 *Cybermerc and Vault Cloud*
16 *Confidential Submission 18*
17 *Telstra Cooperation Limited*

Final Principles: Applying Industry Feedback

The draft Principles published in the public discussion paper were changed through the consultation process. The final Principles reflect the advice received from industry and the community.

Pillar 1: Security-by-design

Security-by-design *Security should be a core component of critical technologies. Organisations should ensure they are making decisions that build in security from the ground-up.*	1. Understand what needs to be protected, **why it needs to be protected and how it can be protected**. 2. Understand the **different** security risks posed by your supply chain. 3. Build security considerations into **all organisational processes, including** into contracting processes, that are proportionate to the level of risk (and encourage suppliers to do the same). 4. Raise awareness of **and promote** security within your supply chain.

Orange text outlines changes following public consultation and feedback incorporated.

The security-by-design pillar received strong support throughout consultation. We heard that it is essential for organisations to understand their critical technology assets, why they need to be protected, and how they should be protected.[18] Organisations should understand the impacts and dependencies their technology supply chains have on their business, customers and the community.

Feedback highlighted that organisations should consider the whole-of-life of the product or service they provide to encourage security across the lifecycle.[19] Security-by-design from a vendor or provider perspective should be a holistic end-to-end approach starting at the product concept phase.[20] We also heard about the importance of organisations understanding what impacts different risks could have on their operations.

A key takeaway from the consultation process is that organisational maturity can play a role in the implementation of these Principles. We heard that not all businesses have the supply chain or cyber security skills or expertise to implement the security-by-design Principles. We heard that further Government guidance is needed to support the implementation of the security-by-design pillar for some organisations.

18 *Telstra Cooperation Limited*
19 *Industry Workshop 1 (26 November 2020)*
20 *Cisco Systems Australia Pty Ltd*

Pillar 2: Transparency

Transparency

Transparency of technology supply chains is critical, both from a business perspective and a national security perspective.

5. Know who **critical** suppliers are and build an understanding of **their** security measures.
6. Set and communicate minimum transparency requirements consistent with existing standards and international benchmarks for your suppliers and encourage continuous improvement.
7. Encourage suppliers to understand **and be transparent in the depth of** their supply chains, and be able to provide this information to **customers**.

Orange text outlines changes following public consultation and feedback incorporated.

Consultation highlighted the importance of the transparency pillar and that two-way information sharing will play a key role in protecting supply chain security.[21] Suppliers should consider an ecosystem approach, where industry partners take responsibility to share information about their supply chain and across various suppliers.[22] Understanding this information will help organisations provide information to their customers on the supply and security of their supply chains, and the products being developed.[23]

Feedback raised questions around how many layers of the supply chain organisations should be aware of under Principle seven. The updated wording outlines that companies should be transparent in how many layers of their supply chain they are aware of. There is no minimum level of depth of supply chain knowledge required, however companies should be able to identify the layers of their supply chain and be transparent about this knowledge.

If there are to be standards and reporting established around the Principles, consultation raised the idea that the regime set out in the *Modern Slavery Act 2018 (Commonwealth)* could be a useful tool to align Government reporting mechanism.[24]

21 *Industry Workshop 2 (1 December 2020)*
22 *Industry Workshop 2 (1 December 2020)*
23 *AustCyber, Standards Australia, Industry Workshop 2 (1 December 2020)*
24 *Cyber Security CRC*

Pillar 3: Autonomy and integrity

Autonomy and integrity

Knowing that your suppliers demonstrate integrity and are acting autonomously is fundamental to securing your supply chain.

8. **Seek and** consider the **available advice and guidance on** influence of foreign governments on suppliers and seek to ensure they operate with appropriate levels of autonomy.
9. Consider if suppliers operate ethically, with integrity, and consistently with international law and human rights.
10. Build strategic **partnering** relationships with **critical** suppliers.

Orange text outlines changes following public consultation and feedback incorporated.

In the autonomy and integrity pillar there was a consensus that not all foreign governments pose the same level of security risk. We heard that to assist in the decision-making process, businesses and organisations should seek available advice and guidance on foreign governments, including what specific considerations of influence or interference should be made.[25] We heard that a risk management approach could be taken when dealing with foreign governments[26] and, that there is a distinction between interference and influence[27]. The changes to the Principles reflect the responsibility of organisations in finding and considering the available advice in this space, including available internal organisational processes.

This is particularly relevant for organisations with multinational supply chains. Feedback indicated that these companies should understand the level of autonomy in which they operate, such as where their data is stored in each jurisdiction and if information is being shared with other foreign governments.[28]

25 *Standards Australia, Confidential Submission 13, Palo Alto Networks, The Software Alliance (BSA), Telstra Cooperation Limited, Industry Workshop 2 (1 December 2020)*
26 *The Software Alliance (BSA)*
27 *Industry Workshop 2 (1 December 2020)*
28 *Industry Workshop 2 (1 December 2020)*

Final Principles

The final Principles are shown below. Further information can be found at www.homeaffairs.gov.au.

Agreed pillars	Agreed Principles
Security-by-design *Security should be a core component of critical technologies. Organisations should ensure they are making decisions that build in security from the ground-up.*	1. Understand what needs to be protected, why it needs to be protected and how it can be protected. 2. Understand the different security risks posed by your supply chain. 3. Build security considerations into all organisational processes, including into contracting processes, that are proportionate to the level of risk (and encourage suppliers to do the same). 4. Raise awareness of and promote security within your supply chain.
Transparency *Transparency of technology supply chains is critical, both from a business perspective and a national security perspective.*	5. Know who critical suppliers are and build an understanding of their security measures. 6. Set and communicate minimum transparency requirements consistent with existing standards and international benchmarks for your suppliers and encourage continuous improvement. 7. Encourage suppliers to understand and be transparent in the depth of their supply chains, and be able to provide this information to customers.
Autonomy and integrity *Knowing that your suppliers demonstrate integrity and are acting autonomously is fundamental to securing your supply chain.*	8. Seek and consider the available advice and guidance on influence of foreign governments on suppliers and seek to ensure they operate with appropriate levels of autonomy. 9. Consider if suppliers operate ethically, with integrity, and consistently with international law and human rights. 10. Build strategic partnering relationships with critical suppliers.