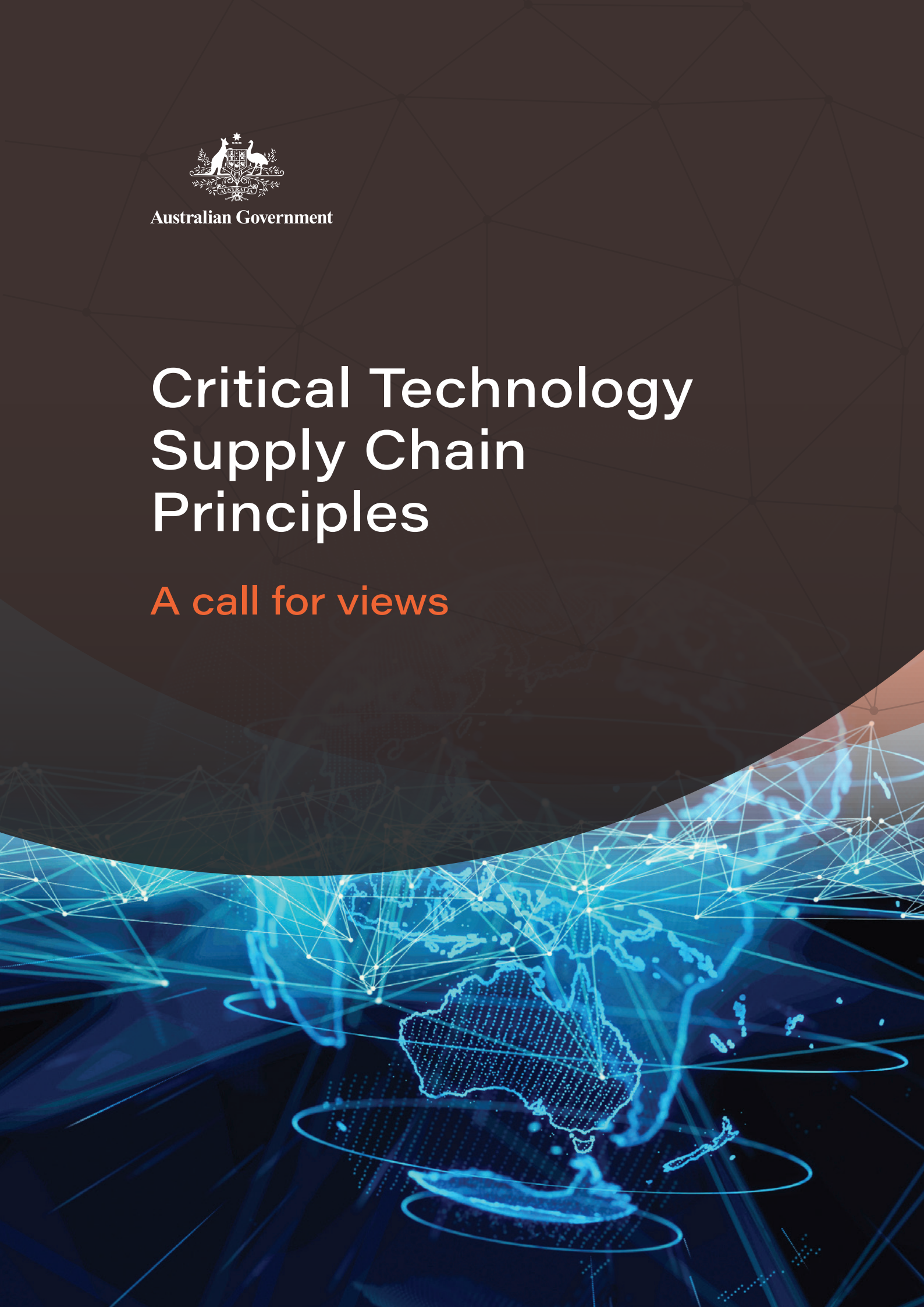
Australian Government

Critical Technology Supply Chain Principles

A call for views

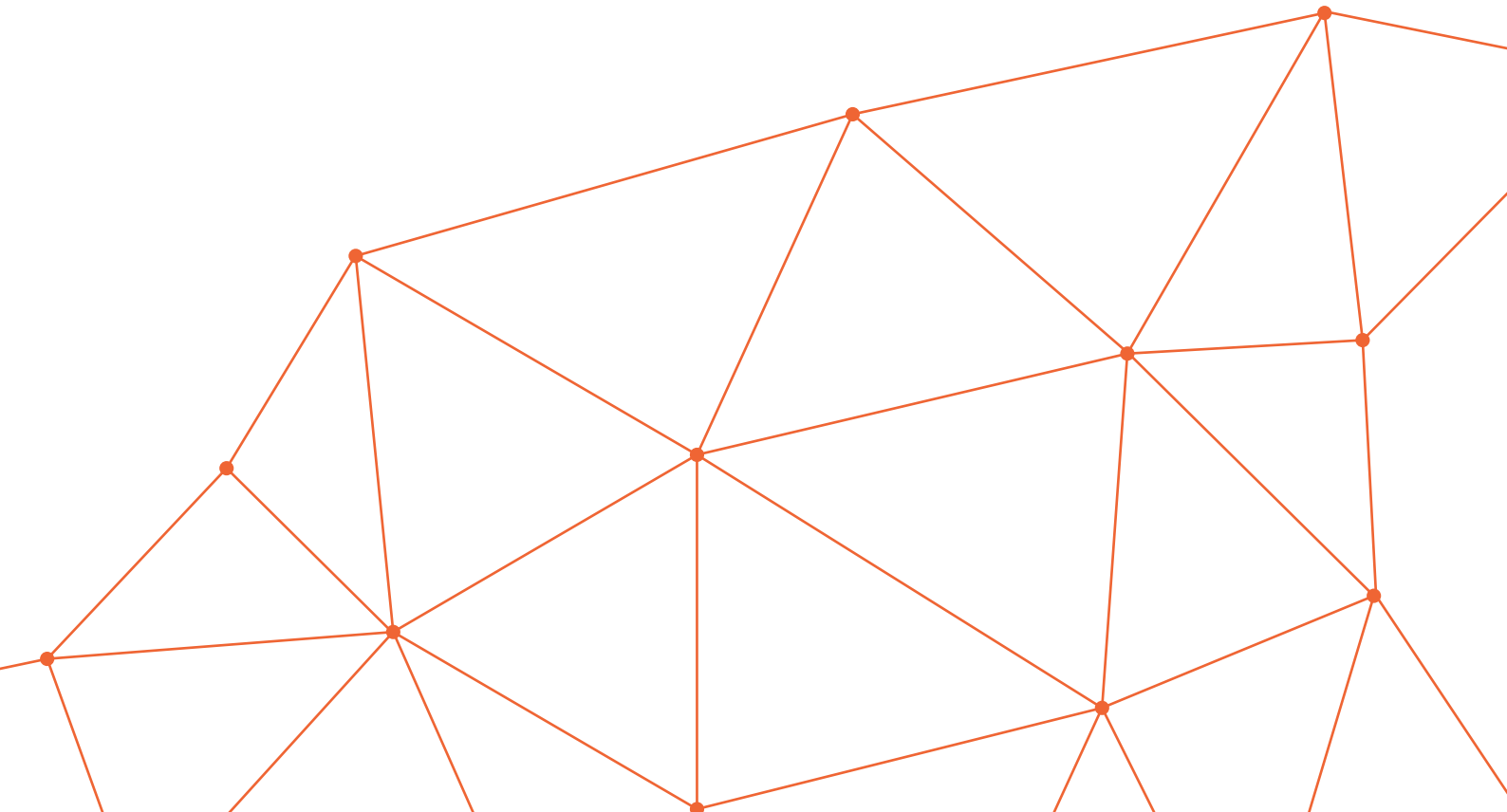


Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Table of contents



Executive Summary

Supply chains for critical technologies in Australia must be more resilient. Australia's COVID-19 experience highlights the vulnerabilities of supply chains for products essential to the country. At the same time, the global technological landscape is evolving at an unprecedented pace and geostrategic competition is affecting how critical technologies are being developed and used.

The more dependent society becomes on technology, the less governments and organisations can rely on traditional habits and decision-making frameworks when it comes to their supply chains. Improving the management of critical technology supply chains specifically, across the economy will help build Australia's resilience to future shocks, as well as address the inherent risks to our nation's national security, economic prosperity and social cohesion.

Advances in technology underpin our future prosperity, however they also expose our nation to more risks. Malicious actors can use critical technologies to harm our national security, and undermine our democracy. One way to address these risks is to consider the supply chains of critical technologies, and how these could be made more secure.

Understanding the risks is the first step towards organisations of all sizes taking action to create diverse, trusted and secure supply chains. That's why the Australian Government is developing the *Critical Technology Supply Chain Principles*. These Principles will be non-binding and voluntary, and are intended to act as a tool to assist governments and businesses in making decisions about their suppliers and transparency of their own products. The Principles will help Australian business consider the unforeseen risks when developing critical technologies, building business resilience.

The suggested Principles will be grouped under three pillars: security-by-design, transparency, and autonomy and integrity. The suggested Principles below align with guidance provided by the Australian Signals Directorate's Australian Cyber Security Centre on supply chain risk management.[1]

1 Australian Cyber Security Centre, 2020, *Cyber Supply Chain Risk Management*, https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management.

The suggested Principles are one tool amongst a suite of other carefully balanced actions the Government could take to shape secure, resilient and trusted technologies and an international environment in which secure technologies support national security, sustainable economic growth, development and stability.

Suggested Critical Technology Supply Chain Principles

Agreed pillars	Suggested 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 and why.
	2. Understand the security risks posed by your supply chain.
	3. Build security considerations into contracting processes that are proportionate to the level of risk (and encourage suppliers to do the same).
	4. Raise awareness of 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 suppliers are and build an understanding of 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 their supply chains, and be able to provide this information to consumers.
Autonomy and integrity *Knowing that your suppliers demonstrate integrity and are acting autonomously is fundamental to securing your supply chain.*	8. Consider the 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 their human rights responsibilities.
	10. Build trusted, strategic relationships with suppliers.

The suggested Principles recognise that security should be a core component of critical technologies, and should be built-in from the outset. This needs to be accompanied by a good understanding of who suppliers are, whether they act with integrity in line with Australian law and human rights responsibilities. These Principles can act as a tool which organisations could employ to lower their risks to unforeseen threats, which could lead to potential reputational damage from using insecure products, loss of IP or customer data or a loss of access to markets.

By choosing to apply the suggested Principles, governments and businesses will be able to better adopt new critical technologies, buy or use products and services with greater confidence and securely realise their full benefits. Other potential benefits include improved supplier relationships, clearer expectations for suppliers, stronger customer confidence that results in a competitive edge, and better resilience in times of crisis.[2]

As a first step, we encourage organisations to apply the suggested Principles to their own operations and their direct suppliers, and carry forward the expectation that those suppliers are doing the same.

2 Business.gov.au, 2020, *Business risks*, https://www.business.gov.au/risk-management/risk-assessment-and-planning/business-risks.

We are seeking your views on the suggested Principles and how we can ensure they are effective in achieving their purpose. We have proposed a series of questions you may wish to answer as you provide your views through the written submission process accessible on the Department of Home Affairs website. You may wish to cover some or all of the following questions:

1. Do you think there is a need for Government to address the security of critical technology supply chains?
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?
3. To what extent is your organisation already applying the suggested Principles?
4. What would the costs and benefits be from applying the suggested Principles in your organisation (e.g. economic, competition, social and environmental)? If possible, please quantify the costs and benefits.
5. What additional advice, guidance or tools would you require from Government to effectively apply the suggested Principles?
6. Do you think your organisation would have difficulties sourcing certain products by requiring your own suppliers to meet the suggested Principles? If so, which products do you think would be most impacted?
7. Are there other standards or expectations in the Government tender process that you believe already address the objectives of the suggested Principles? If so, which ones and are there competing requirements?
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?
9. Is there anything else Government should consider when finalising the proposed Principles?

The Department of Home Affairs and the Department of Industry, Science, Energy and Resources will review the feedback received and use it to ensure the suggested Principles are fit for purpose, benefit those who adopt them and meet industry's expectations of Government leadership. The final Principles will be used by the Australian Government to help guide its own decisions, including procurement, and are voluntary for Australian businesses, states and territories and local councils who wish to do the same. The Principles will then be reviewed 12 months after voluntary implementation.

Context

Australia needs to increase our national resilience

Australia's success as a nation is founded on social cohesion, democracy, an open economy and competitive industries, the safety of our people, and multi-faceted international partnerships. The strength of these foundations underpins our resilience: the ability to withstand and recover from economic, security or social disruptions, crises or shocks.

Our national interest is served by remaining open and connected to the global economy, while continuing to protect our national security and sovereignty. To maximise the national interest, decision-making processes need to consider costs, benefits and trade-offs and remain proportionate to identified risks.

Access to secure critical technologies is fundamental to a prosperous and resilient Australia

Secure critical technologies are fundamental to a prosperous, secure and united Australia. Critical technologies are current and emerging technologies that have the capacity to significantly enhance or pose a risk to our national interest. These technologies can be digital, like artificial intelligence (AI) and quantum computing, or non-digital, like synthetic biology. In addition to considerations about the national interest, we also encourage organisations to think about what technologies are critical to their operations more broadly and how the suggested Principles could apply to make them more resilient. Our ability to harness the opportunities and minimise the risks created by critical technologies is essential to Australia's national interest. Technological advances play an important role in driving productivity, economic growth and improved living standards.

We are an innovative nation that develops new ideas and quickly adopts technology from overseas. Australia is a world leader in key areas of research such as advanced manufacturing, and Australian industry is keen to invest in emerging technologies. However, overseas markets supply many of our technological requirements and Australia imports many technologies and components, that we are not best placed to produce locally. To facilitate increased investment and resilience, we need to ensure enduring access to a diverse, secure and trusted supply of critical technologies.

Open trade and investment, diverse, competitive and open markets, and transparent collaborative research all contribute to our national interest and resilience.

New applications of technology must consider economic opportunities, national security risks and impacts on social cohesion

Advances in technology underpin our future prosperity but also have the potential to harm our national security, economic sustainability, or interfere with our democracy. Disinformation and foreign interference have been enabled and accelerated by new technologies, which are increasingly used for both civilian and military or state purposes.

One example is AI, which provides opportunities to significantly improve our way of life. AI can improve remote healthcare through AI-assisted health diagnostics; defend against malicious cyber activity by identifying suspicious patterns in network data; improve electricity network efficiency by managing the variability of renewable energy supply in an optimal way; and improve business productivity and decision making through better market forecasting and insights. AI systems can also be used against Australia, and to harm our interests such as the use of AI in deepfake videos, or by powering large scale malicious cyber activity.

Our world-class science and technology institutions and businesses can also be a target for malicious activity. These activities can result in theft of intellectual property or technology, undermining Australia's strategic and commercial advantage.

Everyone has a role to play to ensure Australia can safely, securely and efficiently adopt critical technologies

Improving how we manage vulnerabilities and security threats in technology supply chains will help protect against risks to our national security, sovereignty and way of life. Managing the broad security considerations across the lifecycle of critical technological development and throughout the supply chain is one way to begin addressing these risks.

Government has a role to play in assisting society, academia and business to build the right skills and acquire the necessary tools to manage their own risks. This is particularly important as these organisational risks organisations can have flow-on impacts to the broader community and Australia's national interest. These skills and tools are essential to efficiently and effectively adopting critical technologies in a safe and secure manner. We'll also continue to engage in meaningful consultation with industry and the public, and across all levels of government, to manage technology risks.

Actions, such as anti-competitive and predatory behaviour that seek to unduly restrain or eliminate competition and incite adverse effects on trade, economic development or Australia's national interests should be countered. Organisations or state actors engaged in such illegitimate activity should not be supported, and such actions should be discouraged. Making informed purchasing decisions can help ensure such organisations who engage in illegitimate activity are not supported by government.

But Government alone cannot manage all the risks. Industry already manages risks such as Australians' data and privacy as good business practice, and extending this management to critical technologies will serve to protect business IP and data. Further, this management will protect systems against malicious attack and potential reputational damage. Working together, industry and Government will invest in and use critical technologies that are secure to protect Australians, their data, and our national interests. The Principles are also a way for Government to give industry the tools to make business decisions that are informed by its understanding of current threats and geostrategic insights.

Government will take a principles-based approach to set expectations that technology providers act securely, with integrity and in accordance with Australia's legislative and regulatory frameworks. Our goal is to ensure Australians are always able to access safe and secure technologies.

Critical technology supply chains need to be resilient

A key aspect of supply chain security is mitigating risks. Supply chains can be interrupted or distorted by a range of issues, from malicious cyber activity and supplier insolvency through to coercion and international trade disruptions.

Although many businesses are aware of these risks, and may already have strategies in place to combat them, the geostrategic environment of critical technologies and supply chains is changing rapidly. Improving the management of critical technology supply chains across the economy will help build Australia's resilience. This will better position the Australian economy to resist, absorb, accommodate, recover from and transform in the face of any future crisis.

As our economy becomes more reliant on technology, all organisations must have confidence in the security of the products and services they use, whether they be digital or otherwise. The successful adoption of critical technologies are the economic opportunities they offer is dependent on securely and safely integrating them into our societies.

Technology has also become a central element of geostrategic competition, with some states seeking to dominate critical and emerging technologies for strategic advantage. Economic coercion, foreign interference, espionage and disruption of critical services can all be facilitated through technological dominance. Malicious state-based actors can also exploit significant opportunities created by the stress placed on global technology supply chains from the COVID-19 pandemic to pursue critical technology related objectives.

The more dependent society becomes on technology, the less governments and organisations can rely on traditional habits and decision-making frameworks when it comes to their supply chains.

Being resilient to significant shocks depends on having a diverse supply of trusted critical technologies. Ensuring that we always have the capacity to meet Australia's critical needs requires an informed understanding of supply chains and acting to reduce any vulnerabilities. This includes making sure supply chains are transparent, which means understanding how products, including their inputs and related services, are sourced.

Organisations of all sizes need to be able to trust their suppliers. They also need to understand what they are buying and any embodied risks. This relies on an open, transparent, diverse and competitive technology ecosystem, where suppliers build in security-by-design proportionate to the risk and comply with applicable Australian laws.

Resilience can also give organisations an edge over their competitors. Deeper understanding of supply chains may uncover opportunities for an organisation, such as increased flexibility, access to new capabilities, lasting cost savings and higher margins.

Demand exists worldwide for trusted and secure critical technologies, including their components and support services. Businesses who take stronger approaches to supply chain security may benefit from commercial opportunities to export trusted and secure offerings, while also contributing to protecting Australia's national security.

For the economy as a whole, understanding national supply chains builds greater resilience and underpins growth. And in the global economy, no organisation is isolated. If an organisation adopts, uses or relies on a critical technology, it is likely that some aspects of its supply chain are based overseas.

Critical Technology Supply Chain Principles

Security-by-design

Suggested Security-by-design Principles

Appropriate security should be a core component of critical technologies. Organisations can ensure they are making decisions that build in security from the ground up by taking into account the below Principles:

1. Understand what needs to be protected and why.
2. Understand the security risks posed by your supply chain.
3. Build security considerations into contracting processes that are proportionate to the level of risk (and encourage suppliers to do the same).
4. Raise awareness of security within your supply chain.

Security-by-design means a design-stage focus on ensuring that security is built into products and services from the ground up. This is a process of building in appropriate security to protect systems and end users from threats and vulnerabilities. Considering security in the design phase of a product will ensure it is robust to future threats and reduces life-cycle costs. For example, when it comes to digital products and services, this means appropriate security within hardware, firmware and software.

When security is built in by-design it also means customers do not need to have expert knowledge and that they are not unfairly transferred risk that they are not best placed to manage. Similar protections that apply in other sectors of the Australian economy such as road safety or workplace health and safety should also be considered in relation to critical technologies.

Consumers also have a role in ensuring security-by-design. Organisations will always carry some responsibility for their own security, regardless of how secure products and services are made. This starts with choosing products and services that have been made secure-by-design and requiring better security features from suppliers.

Appropriate security helps to prevent critical technologies from being exploited or manipulated by a malicious actor. This will give organisations confidence in their decisions, as well as giving supplier's confidence in the integrity of the products they are making. Not doing so is a business risk, which might be costly to an organisations bottom line or reputation over the long-term. Resilient organisations will see security as an enabler to protect the benefits they gain from innovation, and purchasing decisions as a way to prevent vulnerabilities being embedded in their supply chains.

By choosing to tell suppliers that purchasing decisions will be informed by the need for built-in security, organisations can encourage a broader positive trend towards higher security standards among critical technology suppliers. This will hopefully see suppliers becoming trusted by choice. By 'trusted by choice' we mean suppliers of critical technology pre-emptively uplifting, or developing, the security credentials of their products and services across the full development cycle.

The nature of critical technologies – their complexity, potential societal impact, and pervasiveness – means that trying to mitigate security concerns after the technology has been developed is likely to be more costly, or potentially ineffective. Knowing that security was built-in from the start of the development of a technology gives customers confidence and trust in what they are buying, as they know security was not an afterthought.

In Focus: Public consultation on Australia's Cyber Security Strategy 2020

A nation-wide consultation period was held to inform the development of Australia's Cyber Security Strategy 2020. Between September 2019 and February 2020, the Department of Home Affairs met with more than 1,400 people in each state and territory and received 215 written submissions. In addition to calls for Government leadership, two of the consistent messages we heard during the consultation were:

1. Products and services should have a minimum level of security built-in by design.
2. Greater awareness about the cyber security risks in the products and services they are buying and using is needed.

There was a widespread view that a baseline level of cyber security should be built into goods and services 'by-design', as most consumers aren't best placed to protect themselves from the risks. We heard this would complement other essential efforts such as awareness raising to help Australians better manage risks.

We also heard calls for Government to consider how to better manage cyber security supply chain risks and that Government needs to '*put responsibility back in the supply chain*'.[3] The security-by-design principles will give all organisations a tool to begin addressing the security risks in supply chains.

Implementation considerations

When working towards security-by-design, business could consider the following:

- Domestic guidelines[4] regarding security-by-design for products and services. Following these guidelines could clarify expectations you may have with your supply chains such as whether you would accept the cyber standards your supplier uses, whether your supplier shares results of recent security assessments or whether you could penetration test the product you are acquiring.
- How to best assess your supply chain from the outset. All supplier relationships require consideration, including IT services. Companies can assign risk levels, security controls and processes for monitoring and threat response that reflect the service or product being supplied. Those services or products performing critical functions would require more extensive processes to be put in place.

3 Ontrac Global. September 2019, *Written Submission: Australia's 2020 Cyber Security Strategy*, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020.

4 Domestic, see: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy; https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice; https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents-mitigation-details.

Transparency

Suggested Transparency Principles

Transparency of technology supply chains is critical, both from a business perspective and a national security perspective. Organisations may wish to take into account the following Principles when making decisions regarding their supply chains:

5. Know who your 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 their supply chains, and be able to provide this information to consumers.

Being transparent means explaining clearly to customers what security measures have been taken, which will reduce uncertainty and increase consumer confidence when purchasing products.

Transparency is a key factor in any organisation's ability to manage risks. Understanding your suppliers and networks ensures your organisation is aware of these risks, can identify bottlenecks, and then determine alternative sources of critical inputs when needed. Building in mechanisms to enhance your supply chain transparency from the outset is key. Organisations should always try to understand what they are dependent on so that a shift or disruption in the global landscape does not threaten their viability.

Transparency also means addressing your own security responsibilities. This responsibility has two parts – being transparent about your own processes and security settings to your consumers, as well as setting and clearly articulating minimum security requirements for suppliers and requiring support for security incidents. Greater transparency about product security, data management and business processes also improves institutional trust. Governments also need to understand the major economic, national security and social implications that depend on, or will depend on, critical technologies. Global technology supply chains are increasingly complex. Organisations should try to avoid vendors who do not understand, or intentionally obscure, their supply chains, particularly if there are more transparent alternatives available. As consumers make more informed decisions, businesses that promote security and transparency will become more highly sought after. By developing the proposed Principles, we also want to be more transparent with Australians and businesses about the drivers for purchasing trusted critical technology offerings.

In Focus: Supply chain transparency during COVID-19

Transparency in supply chains has long since been an issue recognised by business in areas beyond critical technologies. Due to the rapidly changing global technology environment, it is important that this careful management is extended into the development of critical technologies.

Lessons from Australia's COVID-19 experience may also apply to critical technologies. The COVID-19 pandemic brought issues such as sovereign capability to the forefront and demonstrated Australia's dependence on foreign supply chains for a range of essential items we need in a crisis.[5]

COVID-19 particularly exposed the lack of transparency in Australia's manufacturing equipment supply chains. A lack of transparency and increased global demand for medical devices made it difficult to plan and police the risk of procuring substandard or unethical supplies.[6] Agility was demonstrated by a consortium of manufacturers who adapted their manufacturing processes and found alternative sources of supply to produce 2,000 critical ventilators during the crisis.

Implementation considerations

When working towards more transparent supply chains, organisations could consider the following:

- Understanding what you are protecting and why, as well as the inherent risks in your supply chains. Consideration also needs to be given to who your suppliers are and their security measures.
- Mechanisms to promote transparency, including setting minimum security requirements for suppliers, providing support for security incidents, and developing strategies to raise awareness, communicate security requirements and disclose vulnerabilities and/or disruptions.
- Processes to build assurance and develop a culture of continuous improvement.

5 The Hon Karen Andrews MP, May 2020, *National Press Club Address – Canberra*, https://www.minister.industry.gov.au/ministers/karenandrews/speeches/national-press-club-address-canberra.

6 University of Melbourne, August 2020, *More Transparency Needed in PPE Supply Chains*, https://pursuit.unimelb.edu.au/articles/more-transparency-needed-in-ppe-supply-chains.

Autonomy and integrity

Suggested Autonomy and Integrity Principles

Knowing that your suppliers demonstrate integrity and are acting with autonomy is fundamental to securing your supply chain. As such, organisations can take into account the following Principles:

8 Consider the potential influence of foreign governments on suppliers and whether they operate with appropriate levels of autonomy.

9 Consider if suppliers operate ethically, with integrity, and consistently with their human rights responsibilities.

10 Build trusted, strategic relationships with suppliers.

Autonomy and integrity means the ability for an organisation to operate at its own direction according to its own drivers as well as without undue external influence that may jeopardise the security of its products or services.

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. This includes considering the potential for foreign government influence in your supply chain, and how this supplier could access your systems and sensitive data.

Knowing that your suppliers demonstrate integrity and are acting with autonomy is fundamental to securing your supply chain. Due to the nature of critical technology development and manufacturing, it is likely that you will have some vendors in your supply chain that are located or source their own inputs outside of Australia, which could introduce vulnerabilities to your business.

Consideration should be given to the level of foreign government influence or direction over organisations responsible for or involved in critical technologies in Australia. Decision makers should also consider whether these factors could result in actions that would run counter to Australia's national security or conflict with Australian laws. This includes whether an organisation is likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law. The integrity in their product origins, certifications, and trajectory should be clear and understandable. If a foreign supplier's activities are found to breach Australian law, organisations should report the activities to appropriate authorities and reconsider using these suppliers.

Suppliers should demonstrate integrity in their delivery and use of critical technologies. Supply chain integrity can be undermined by illegal supplier practices that are often unknown to the purchaser at the procurement stage or during the course of the contract.[7] The integrity of their product origins, certifications, and trajectory should be clear and understandable.

7 Australian Department of the Treasury, March 2019, *Black economy – increasing the integrity of government Procurement*, https://treasury.gov.au/sites/default/files/2019-03/p2019-t369466_0.pdf.

In Focus: Australian Government 5G security guidance

In 2018, the Australian Government provided 5G security guidance to Australian carriers. Due to the critical and enabling nature of 5G technology, the Government undertook an extensive review of the national security risks to 5G networks, to safeguard the security of Australians' information and communications.

The Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference.[8]

Implementation considerations

Risk assessments of suppliers' products should take into account all relevant factors, including applicable legal environment and other aspects of supplier's ecosystem. These factors may be relevant for your organisation to maintain a high level of supply chain security.

When working towards making sure critical technologies are supplied by autonomous and secure enterprises acting with integrity and in line with Australian laws, organisations could consider the following:

- Whether certain actors are known to be conducting espionage against your sector or suppliers. The Centre for Strategic and International Studies[9] issues alerts regarding a foreign government's cyber espionage.
- Whether there is evidence of board member involvement in criminal activity or whether any board members have previously declared bankruptcy.

Following these suggested Principles will increase consumer trust and confidence in products and services supplied by business.

8 Senator the Hon. Mitch Fifield and The Hon. Scott Morrison MP, August 2018, *Media Release: Government Provides 5G Security Guidance to Australian Carriers*, https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/6164494/upload_binary/6164494.pdf;fileType=application%2Fpdf#search=%22media/pressrel/6164494%22.

9 Centre for Strategic and International Studies, 2020, *Significant Cyber Incidents*, https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

Annex A: Glossary

Consumers – A person to whom goods or services are or may be supplied by participants in the industry. This includes all Government entities, all state, territory and local councils. This also includes all sellers to Government through the Digital Transformation Agency's whole of government panel arrangements, marketplaces and volume sourcing arrangements.

Critical technology – Current and emerging technologies that have the capacity to significantly enhance or pose a risk to our national interest (prosperity, social cohesion or national security).

Emerging technology – Technologies that are currently developing, or that are expected to be available within the next five to ten years

Risk – The graded severity of impact to security through realisation of a vulnerability by a threat.

Risk owner – The owner of the final critical technology product is the ultimate owner of risk to that system. Risk owners should be aware any untreated risk is transferred to others who depend on the system or business.

Supply chain – Supply chain includes the linked processes of design, manufacture, supply, delivery, support and decommissioning of equipment or services that are utilised within an organisation. A critical technology supply chain can include vendors, service providers, manufacturing facilities, logistics providers, distribution centres, distributors, wholesalers, and other organizations involved in the manufacturing, processing, design and development, handling and delivery of the products or services

Supply chain assurance – Confidence that the supply chain will produce and deliver elements, processes, and information that function as expected.

Supply chain risk – The combination of vulnerabilities in an organisations supply chain, the threats that organisations supply chain is likely exposed to, and the impact of a realised vulnerability by a threat.

Supply chain risk management – A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

Supplier – Organisation or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain. Includes (i) developers or manufacturers of information systems, system components, or information system services; (ii) vendors; and (iii) product resellers.

Technology – In the context of this paper, technology means the combination of skills, systems, processes, techniques and knowledge in the development of new products and services.

Vendor – Typically the organisation that supplies a product or service to the customer.

Vulnerability – A weakness in a system that can be exploited by a threat, ultimately compromising the security of the system.

Further information and definitions are available at https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management-practitioner-guide and https://csrc.nist.gov/glossary?index=V.

Annex B: Existing frameworks, principles and guidelines

When introduced, the Principles will complement other existing Government efforts to ensure the resilience of supply chains. This is a non-exhaustive list of the information currently available on supply chain resilience, but provides a broad perspective of how Government is currently addressing supply chain risks.

Australian Industry Participation Plan

Australian Industry Participation (AIP) requirements ensure full, fair and reasonable opportunity for Australian industry to compete for work. This includes work in major public and private projects in Australia, and procurements or projects receiving Australian Government funding of $20 million or more.[10]

The AIP requires business to detail the way in which they intend to engage Australian Industry in their project. The content of the AIP includes identification of key goods and services to be acquired for the project which act as a precursor to understanding the supply chain and identifying vulnerabilities.

Cyber Security Requirements

Through the Australian Cyber Security Centre, the Australian Government provides a range of cyber security advice for business to consider. This includes:

- Cyber Supply Chain Risk Management Framework.[11]
- Information Security Manual.[12]
- Essential Eight.[13]

Protective Security Policy Framework

The Protective Security Policy Framework administered by the Attorney-General's Department assists Australian Government entities to protect their people, information and assets and is applied to all government tenders. The Protective Security Policy Framework primarily contains guidance for businesses on how to ensure the goods they supply to government are secure, however it is a useful resource when extended to supply chains.

Defence Industry Requirements

Industry supplying to the Department of Defence will also have a range of standards applied as requirements in the tender process including the Defence Industry Security Program, and may already be addressing the Principles.

Defence has also outlined the Government's long-term vision to build and develop a robust, resilient and internationally competitive Australian Defence industrial base that is better able to help meet Defence capability requirements through the 2018 Defence Industrial Capability Plan. This is another mechanism used to invest in secure, transparent Australian supply chains.

Foreign Investment Review Board

The Foreign Investment Review Board (the Board) is a non-statutory body established in 1976 to advise the Treasurer and the Government on Australia's Foreign Investment Policy (the Policy) and its administration.

The Board's functions are advisory only. Responsibility for making decisions on the Policy and proposals rests with the Treasurer. The Treasury's Foreign Investment Division (the Division) provides secretariat services to the Board and is responsible for the day to day administration of the arrangements.

10 Department of Industry, Science, Energy and Resources, December 2019, *Australian industry participation*, https://www.industry.gov.au/regulations-and-standards/australian-industry-participation.

11 Australian Cyber Security Centre, 2020, *Cyber Supply Chain Risk Management*, https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management.

12 Australian Cyber Security Centre, 2020, *Australian Government Information Security Manual (ISM)*, https://www.cyber.gov.au/acsc/view-all-content/ism

13 Australian Cyber Security Centre, 2020, *Essential Eight Explained*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-explained

The role of the Board, including through its secretariat, is to:

- examine proposed investments in Australia that are subject to the Policy, the Foreign Acquisitions and Takeovers Act 1975 (the Act) and supporting legislation, and to make recommendations to the Treasurer and other Treasury portfolio ministers on these proposals;
- advise the Treasurer on the operation of the Policy and the Act;
- foster an awareness and understanding, both in Australia and abroad, of the Policy and the Act;
- provide guidance to foreign persons and their representatives or agents on the Policy and the Act;
- monitor and ensure compliance with the Policy and the Act; and
- provide advice to the Treasurer on the Policy and related matters.[14]

Foreign Influence Transparency Scheme Act 2018

The Attorney-General's Department manages the *Foreign Influence Transparency Scheme Act 2018*. The scheme came into effect in 2019 and although not focussed on critical technologies, the scheme may provide some means of determining foreign influence in certain circumstances. This Act is applied across government tenders however does not apply a deep supply chain assessment in the development of critical technologies.

Security of Critical Infrastructure Act 2018

The Department of Home Affairs' Critical Infrastructure Centre (CIC) administers the *Security of Critical Infrastructure Act 2018* (the SOCI Act), which imposes reporting obligations on owners and operators of critical infrastructure assets, and permits the Minister for Home Affairs to direct action in relation to those assets in limited circumstances.

Home Affairs is currently progressing work on a reform package that will seek to build upon these existing measures, and broaden the scope of the SOCI Act to capture certain assets in the Education, Research and Innovation sector (amongst other areas). A key component of the reforms is the *positive security obligation* which would require operators of critical infrastructure assets to proactively identify and mitigate a range of risks, which may include supply chain risks.[15]

Australian Trusted Trader Program

Australian Trusted Trader reduces red tape for Trusted Traders at the border, improves certainty in export markets, and expedites the flow of their cargo in and out of Australia, which means faster access to market. Administered by the Department of Home Affairs with the Australian Border Force, Trusted Trader is free and accredits Australian businesses with compliant trade practices and a secure supply chain. Once accredited, businesses have access to a growing range of benefits that simplify their customs processes.[16]

International Frameworks

In order to maintain pace with international counterparts and capitalise on export opportunities, Australia needs to address the vulnerabilities in our critical technology supply chains. Globally, nations have moved to consider supply chain vulnerabilities more closely in the wake of COVID-19. The United Kingdom[17] and New Zealand[18] have both released supply chain security principles, which provide high level advice to business.

The United States and the European Union have also signalled their intent to introduce greater diversity and trust within critical technology markets. The United States released a supply chain security strategy in 2012, but are yet to provide business specific advice.

Australia is not alone in addressing the risks new critical technologies create, while seeking to capitalise on the opportunities they present. The proposed Principles are one way the Australian Government is contributing to being a trusted and influential partner on critical technologies in the international community.

14 Australian Foreign Investment Review Board, 2020, *About FIRB*, https://firb.gov.au/about-firb.
15 Further detail on the proposed reforms are available here: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems.
16 Australian Border Force, 2020, *Australian Trusted Trader*, https://www.abf.gov.au/about-us/what-we-do/trustedtrader.
17 United Kingdom National Cyber Security Centre, 2020, *Supply chain security guidance*, https://www.ncsc.gov.uk/collection/supply-chain-security.
18 New Zealand Government, 2018, Principles of supply chain security, https://www.protectivesecurity.govt.nz/governance/supply-chain-security/principles-of-supply-chain-security/.