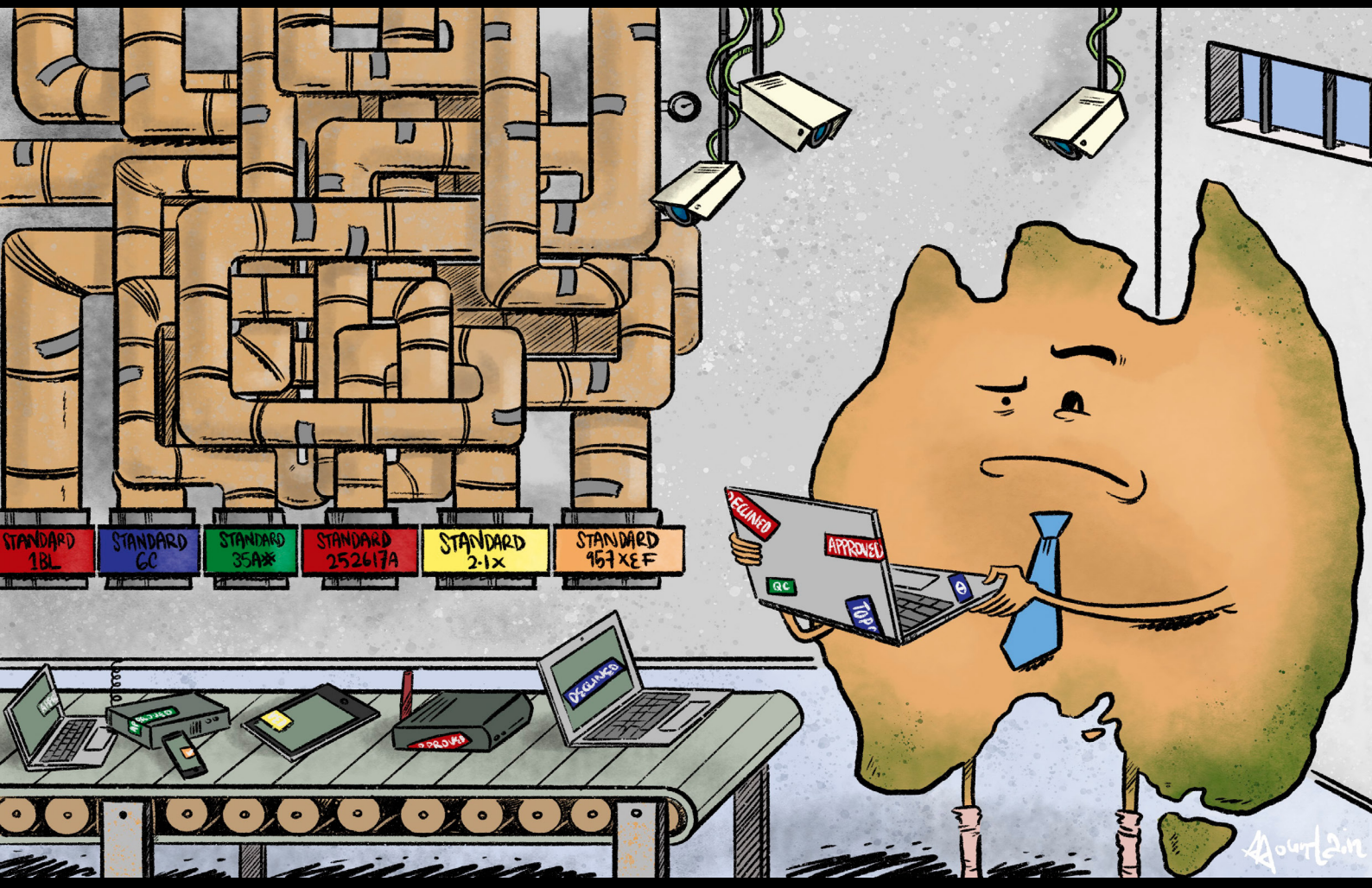
Working smarter, not harder

Leveraging government procurement to improve cybersecurity and supply chains

Rajiv Shah



ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE
macquarie GOVERNMENT

Policy Brief
Report No. 27/2020

About the author

Rajiv Shah is a Fellow at ASPI's International Cyber Policy Centre. He has worked in the cyber, intelligence and security business for more than 20 years, over which time he has seen the internet evolve from an academic curiosity to today's hyperconnected world. He has held a broad range of senior leadership roles with major multinational companies and now also leads his own consulting business, MDR Security, providing expert advisory services to government and businesses to grow capacity and capability through building effective and mutually beneficial partnerships. He is also a regular speaker at industry conferences and contributor to industry publications.

Rajiv's experience has spanned a broad range of business and technical domains, with roles that have included business analysis, technical architecture, program delivery, operational management, strategy, business transformation, client relationship management and more. He has spent time working in the UK and the US, and since 2011 has been based in Canberra, Australia.

Before joining the commercial world, Rajiv completed a PhD in quantum physics and retains a keen interest in mathematics and science.

Acknowledgements

The author would like to acknowledge the support of several Australian Government departments that were consulted for this study, in particular the Department of Human Services, along with other industry stakeholders who took time to share their experiences and perspectives. ASPI's International Cyber Policy Centre receives funding from a variety of sources including sponsorship, research and project support from across governments, industry and civil society. ASPI would like to acknowledge Macquarie Government for supporting this research project.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber and emerging technologies and their impact on broader strategic policy. The ICPC informs public debate and supports sound public policy by producing original empirical research, bringing together researchers with diverse expertise. To develop capability in Australia and our region, the ICPC has a capacity-building team that conducts workshops, training programs and large-scale exercises in Australia and overseas for both the public and private sectors. The ICPC enriches the national debate on cyber and strategic policy by running an international visits program that brings leading experts to Australia.

Important disclaimer

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published August 2020

Cover image: Illustration by Wes Mountain. ASPI ICPC and Wes Mountain allow this image to be republished under the Creative Commons License Attribution-Share Alike. Users of the image should use the following sentence for image attribution: 'Illustration by Wes Mountain, commissioned by the Australian Strategic Policy Institute's International Cyber Policy Centre.'

Funding for this report was provided by Macquarie Government

Working smarter, not harder

Leveraging government procurement to improve cybersecurity and supply chains

Rajiv Shah

Policy Brief
Report No. 27/2020

Contents

What's the problem?

Australian governments are the nation's largest spenders on ICT, but they're failing to maximise the leverage that market power gives them to drive improved cybersecurity and more secure supply chains. Government can harness its spending power to not only improve its own cybersecurity, but to drive better cybersecurity throughout the wider economy. However, current approaches are fragmented and having limited impact, so a concerted national effort is needed, underpinned by major strategic changes in approach.

What's the solution?

The Australian Government and the state and territory governments should establish a single coherent set of security standards expected from suppliers. The standards need to be more than just a tick-the-box exercise to set a minimum standard—they should provide multiple levels through which suppliers can seek to progress by continuous improvement. In order to protect sensitive data, secure managed enclaves should be used to minimise exposure to the risks of individual suppliers' ICT systems. Procurement frameworks need to provide commercial incentives for suppliers to improve their security. In limited areas where there's a compelling strategic benefit to Australia from building capability, those frameworks should also be linked to a sovereign capability framework to ensure that preference is given to Australian companies.

Introduction

It's forecast that this year there will be more than two and a half times more connected devices than there are people.[1] Securing those devices and networks is critical but increasingly challenging—in 2018–19, the Australian Cyber Security Centre (ACSC) responded to 2,164 incidents,[2] while data from the ReportCyber network suggests that more broadly across Australia there are approximately 150 cybercrime incidents per day.[3]

The Australian Government allocated an average of $65 million per year to its cybersecurity strategy over the past four years, but that figure is dwarfed by broader federal government ICT procurement, and even more so by the combined ICT spend by the three levels of Australian government. The amount spent annually by the federal government alone has grown significantly from $5.9 billion in 2012–13 to almost $10 billion now.[4] State and local governments are also big spenders on ICT: the NSW Government IT budget is over $3 billion per year.[5]

Such scale means that government ICT procurement has significant market power. This paper explores how that procurement could be leveraged as part of the updated cybersecurity strategy currently being prepared for the next four years. The paper starts by examining supply-chain risks and opportunities, before looking at the key barriers and challenges and suggesting how they could be addressed.

This study is based on interviews with key stakeholders in government and industry and a review of openly available material on government procurement approaches. While the focus is on Australian Government procurement, state and local government procurement is considered where appropriate.

Supply-chain risks and opportunities

Supply chains are integral to cybersecurity. Almost all end users of ICT systems rely on hardware, software or services built or delivered by someone else. Where a supplier becomes a critical node in the supply chain, integral to a large part of the ICT ecosystem, security failures have the potential to generate major systemic cyber and operational risks. We rely on suppliers exercising due diligence in their development, management and operational activities to avoid deliberate or accidental compromise (see box).

Supply-chain assurance risks

The first priority for government ICT procurement should be to ensure the security of the supply chain. However, it's clear that supply-chain assurance can mean different things to different people. Generally, it can be considered under three main themes, which aren't mutually exclusive:

- **Trust in the supplier company or organisation:** Who owns, controls or influences the supplier? For nationally sensitive cases, there may be a preference or mandate for Australian-based capabilities. For example, the Digital Transformation Agency hosting strategy sets standards for data sovereignty and facility ownership, not just when contracts are signed, but throughout the lives of contracts.[6]
- **Security of the supplier's IT systems:** What controls does the supplier have in its IT systems to protect data received from the government customer or generated as part of delivering the contract? This can become important when suppliers are given access to the customer's IT systems even for limited purposes. One of the highest profile data breaches—the loss of 70 million credit card details by Target in the US in 2013—occurred through the compromise of the IT systems of one of Target's refrigeration contractors, which had access to a supplier portal for submitting invoices.
- **Security of the products and services being delivered by the supplier:** Assuring the ownership of a company and its internal IT doesn't necessarily mean that the products and services delivered won't have security vulnerabilities. That will depend on the supplier's security design and the assurance applied in their delivery. For example, this is critically important when procuring cloud services—the security of any applications that are run 'in the cloud' depends on the security of those individual applications.

The problem is that, in a market economy, the market often doesn't provide the right incentives to suppliers. No one buys telecommunications services based on security, and how many consumers even think about the security options provided by their internet-connected doorbell? Governments are reluctant to directly intervene in the market, due not only to the cost and complexity of doing so, but also the moral hazard created by taking responsibility for decision-making away from the private sector and creating the perception that government is responsible for any residual risk.

However, government does interact with the private sector through its very significant procurement activities. Its position as a major buyer potentially provides significant market power that could be used to address some of these challenges. In an environment in which resources for cybersecurity are very limited, this could have the advantage of leveraging other existing budgets for ICT procurement. Of course, the priority should be to ensure security for the direct purposes of the procurement, but government also has an opportunity to leverage its market power to provide for broader benefits to the Australian economy and society.

Setting security standards expected from its suppliers may help to lift standards across the board. Companies will be incentivised to lift their standards in order to qualify to do business with the government, and it will often be easier for them to apply those standards across their whole enterprises rather than just for their government contracts. One example from a parallel field is the implementation of quality management systems brought about by government departments mandating ISO 9001 certification for suppliers. That has encouraged companies to implement quality management systems and to have them regularly audited and certified. This has created a vibrant market for auditors and consultants to help with designing and implementing appropriate systems and benefited the companies' other customers through better quality assurance of their products and services. In the construction industry, the government has gone even further: companies are obliged to comply with the requirements of the *Code for the Tendering and Performance of Building Work 2016* across their businesses or risk being barred from bidding for federally funded projects.[7]

With the right approach, there's a real opportunity to stimulate innovation and new developments. If government can define the security outcomes required, that can encourage suppliers to compete to develop the most effective and value-for-money approaches to delivery. The most innovative approaches can then provide a market differentiator for the supplier that helps them to build business in the private sector, the export market, or both.

Challenges and barriers

Challenges and barriers to effective ICT supply-chain security include lack of coordination, unclear standards, a fragmented approach to security accreditation, uneven access to the market for suppliers and the need to comply with requirements to provide value for money.

Lack of a coordinated approach

Government procurement of ICT covers a vast range of products and services with different security implications, from commodity hardware for everyday use to highly sensitive specialist defence and national security systems. The Australian Government's ICT expenditure is also spread across approximately 200 departments and agencies, which typically make their own procurement decisions based on their requirements and priorities. Overall governance is provided by the Department of Finance (for example, through the Commonwealth Procurement Rules[8]). The Digital Transformation Agency (DTA) has also negotiated government-wide contracts with key global suppliers,[9] although departments and agencies are not compelled to use those suppliers. This fragmentation hinders efforts to use the combined market power of government procurement. In seeking more coordinated approaches, care will be needed to avoid the pitfalls that the DTA has faced in trying to set up government-wide frameworks.

Security standards and requirements

The Commonwealth Procurement Rules mandate the consideration of security risks in procurement, and it appears that the mandate is being applied. A study by IDC of global procurements for IT hardware showed that Australia performs better than many of its peers, and notably was the only country where there were no examples of ICT hardware procurements that didn't specify any security requirements.[10] Analysis for this report (see box) supports that conclusion but also shows that suppliers need to be ready to comply with a broad range of requirements. It also shows room for improvement for tenders that aren't for direct ICT procurement but may have a key dependency on the security of suppliers' systems to protect sensitive data.

Those working on defence projects often face the most significant risks and sophisticated threats, so for many years the Defence Industry Security Program has been in place to provide assurance of defence suppliers. The program has recently been overhauled to address the market barriers that it created and to implement options for different levels of assurance for different aspects of security, such as personnel, facilities and ICT, appropriate to the nature and sensitivity of the work.

Outside of Defence, requirements are generally more 'light touch', reflecting the different level and nature of risk, but are also much more fragmented and complex. From our analysis the standards that vendors may be asked to comply with, or at least be aware of, include the following:

- The Protective Security Policy Framework (PSPF),[11] issued by the Attorney-General's Department, articulates government protective security policy, covering not just information security but also governance, personnel and physical security. This is quite high level, articulating five principles and 16 requirements to achieve the desired outcomes.

- The *Information security manual* (ISM),[12] issued by the ACSC, is a detailed cybersecurity framework for IT and security professionals. It consists of more than 180 pages and includes hundreds of controls tailored for different levels of government classified material, from 'OFFICIAL' to 'TOP SECRET'.
- Other guidance from the ACSC includes the Essential Eight Maturity Model,[13] which is intended to provide a more manageable list of the top 8 recommended measures that can be implemented to improve cybersecurity, which are themselves a subset of 38 proposed strategies.[14]
- ISO 27001 is an international standard for an information security management system (rather than specific controls).[15]
- PCI-DSS is a specific set of standards for the secure storage and processing of payment card information.[16]

Review of government tender documents

On one day in February 2020, 126 open approaches to the market were published and available on the Australian Government's AusTender website.[17] Of those, 18 were for the procurement of ICT products and services. All of them had some mention of security in the requirements, but the level of detail and approach differed:

- Two didn't specifically mention the PSPF or the ISM, and included vague, very high-level statements; one referred to no security requirements other than personnel screening.
- Twelve specified the ISM and, in most cases, the PSPF. They were supplemented by additional requirements generally appropriate for the nature of the project. However, confusingly, sometimes specific ISM requirements were also called out as separate requirements. Of those 12, four included specific requirements for suppliers to ensure the security of their own supply chains; six were Defence projects referencing specific Defence security frameworks and requirements.

Other standards mentioned included other Australian Signals Directorate (ASD) guidance such as *Strategies to mitigate cyber security incidents*, ASD cryptographic evaluation, NIST–801 and ISO 27001. There were also a number of general statements about the required level of security, which varied from 'reasonable efforts' to mandated use of the 'best available security'. There was inconsistency within individual tenders; for example, in one case requirements for security patching were mentioned in six different places, but the required timescales were variously described as '48 hours' or 'as required' or weren't specified.

Many of the other open approaches to market that were not directly ICT related still appeared likely to involve sensitive data being handed over to the successful contractor to allow it to deliver the required outcomes. Four were selected for review based on the likelihood that they involved the most sensitive data (financial data, personnel data for training, personal details of customers and health data). Of those, one had no security requirements, one mentioned only the need for personnel security screening, one mentioned a general need for compliance with the PSPF and awareness of the ISM, and one required compliance with a number of other standards, including PCI-DSS.

While these standards often have the same objectives, they take different approaches; for example, in whether they specify governance approaches, technical controls or expected security outcomes. It's expensive and time-consuming for suppliers to go through a different process for each tender to prove compliance. A more efficient approach that would improve market dynamics would be to shift to a smaller, simplified set of standards. The DTA has tried to bring some standardisation into digital service delivery by government but has made limited forays into security.[18] However, that may be appropriate, given DTA's procurement focus; cybersecurity requirements should be specified by the appropriate experts and supported by procurement processes, not vice versa.

Furthermore, to be effective, the practical implementation challenges should be considered when choosing appropriate standards. In an attempt to find quick solutions from a buyer's point of view, it appears that standards may be being recycled in different contexts. For example, many of the strategies recommended by ASD were originally formulated as recommendations for government departments and agencies. Although they've subsequently been broadened and recommended to businesses, too, applying them in a small business that doesn't have the governance, policy and processes of a public-sector organisation can be very difficult. The Defence Industry Security Program requires even its smallest suppliers to comply with all of the 'top 4' controls, yet Australian National Audit Office reports regularly show that even many government departments can't meet that threshold.[19] ASD does provide specific guidance for small businesses,[20] although we haven't seen that guidance mentioned in the context of requirements for a government procurement.

There will be a need for experts who understand the practical implementation of the standards, both in the organisation that's procuring the services and in the supplier that's seeking to comply with the standards. Without that advice, expecting suppliers to simply follow the standards is unlikely to achieve the required security outcomes.

Security assurance of products and services procured

While assurance of suppliers and their IT systems is important, especially where sensitive data is being handed over to suppliers, the above standards still don't really provide assurance when purchasing a product or service that it will be secure. This can be addressed by including specific requirements in the contract, but that doesn't address the problem of verifying compliance. For more basic systems, it may be straightforward to verify configurations, safeguards, features and so on, but that's more difficult for complex solutions, including software applications and cloud services. What about cybersecurity products themselves—how can buyers be assured that they behave as claimed and will have the desired security impact?

ASD has for the past few years awarded certification to some cloud services providers for processing data at 'UNCLASSIFIED-DLM' and 'PROTECTED' levels.[21] This was a positive initiative by the appropriate technical experts in government to inject cybersecurity checks into the supply chain, and it has undoubtedly helped the take-up of cloud services by government departments by providing a 'stamp of approval'. However, as it expanded beyond the initial focus on 'infrastructure as a service' into more complex cloud services such as 'platform and software as a service', demand seems to have exceeded the resources that ASD can provide, and it's recently been confirmed that the scheme is being wound down.[22] The announcement from ASD suggests that this will improve opportunities for local Australian

businesses by removing a potential barrier. While the current list includes major multinational hyperscale cloud companies, we understand that some smaller providers have been waiting several years to go through this process, and the list hasn't been updated for over a year. However, pushing the onus onto individual agencies and departments to make their own individual assessments runs the risk of fragmentation.

ASD also runs the Australasian Information Security Evaluation Program (AISEP), which certifies products in order to protect systems and information against cyber threats and lists them on the Certified Products List. This scheme uses an internationally recognised standard, the Common Criteria,[23] with different levels of assurance based on impact, and ASD is also committed to the development of collaborative 'protection profiles' to further broaden the applicability of this scheme. Product vendors must fund their own evaluations, which are carried out by an independent accredited test facility, and ASD oversees the process. However, where cryptographic evaluation is required, that's done internally by ASD, and this can act as a bottleneck in the process due to a shortage of ASD resources. Given the importance of sovereign assurance of this aspect, additional resources should be found, potentially through engaging an external partner if one isn't available internally.

Access to market

Cybersecurity is emerging as one of Australia's most promising growth opportunities and has produced a number of vibrant companies and innovative ideas.[24] Those companies need to connect with initial customers to validate their capabilities and provide a credible customer reference for broader sales efforts. Government contracts could be a good opportunity to do that and are potentially even better than grant funding, but it's difficult for smaller companies, especially new entrants, to gain visibility and access to market opportunities. Many procurements are made through inflexible panel arrangements, forcing procurement to be routed through a handful of suppliers, and panel refreshes take place seldom, if at all, during a 3–5 year time frame. Procurement initiatives to reduce numbers of vendors and the bundling of projects as large integrated work packages are also factors that limit the ability of smaller players to directly tender for work. This means that small businesses may need to sell through a major prime, giving up 15–20% of revenue, which might be the difference between profitable and unprofitable work.

Even if they do get access to respond directly to requests for quotes, smaller companies may struggle to get brand recognition, while decision-makers prefer recognised brand names. Of course, to some extent this is in recognition of the fact that large multinationals can invest heavily in security, but it's notable that many security companies that receive large venture capital investments seem to spend much of them on marketing, such as airport display advertising. There needs to be an even playing field to allow government buyers to assess and compare the security of the products and services being offered by companies of different types and sizes, by assessing against common standards and avoiding ratings based just on perceived brand reputation.

The value-for-money challenge

The Commonwealth Procurement Rules mandate value for money, but it's currently difficult, if not impossible, to put a value on security. Agencies can stipulate minimum mandatory security

requirements, but that doesn't allow suppliers to differentiate themselves—customers and suppliers said that their expectation was that normally the winner would be the lowest cost solution that meets the minimum standards. Of course, for the most sensitive projects there may be more weighting on the security assessment, but that appears to be the exception rather than the rule. If providers believe they have differentiating security capabilities, their only realistic route is to lobby buyers before tender documents are drafted to get their preferred requirements included in the specification (once again, something that's easier for larger established companies to do).

A better alternative would be a mechanism that mandates that security should always be explicitly included in the evaluation. One suggested option has been to explicitly include security as a 'fourth pillar' in evaluating proposals, alongside cost, quality and timescales, although this then leaves subjectivity about how to measure security and weight it against the other criteria. A better approach would be an effective pricing mechanism, reflecting the fact that better security should equate to lower financial risk. We understand that governments have been looking at how to value cybersecurity risk and found it challenging, so little progress has been made on this to date.

Of course, there's a well-established market that provides a mechanism for consolidating data, sharing risk and best practice, helping organisations to manage and reduce risk, and putting a price on the residual risk—the insurance industry. However, the market for cybersecurity insurance, particularly in Australia, is currently poorly developed.[25] Major players are still working out how traditional insurance concepts work in a cyber world where there are different threats (from petty criminals to nation states), attribution is difficult and collateral impacts can be significant. One example is the case of Mondelez v. Zurich Insurance, in which the insurer refused to pay out for the costs of a major cyberattack attributed to nation-state conflict, citing 'act of war' exemption clauses.[26] There could be concerns that having insurance cover might make companies more complacent about security, and even make them more attractive targets for attackers if it's known that they're covered to pay out ransoms to recover encrypted data.

Recommendations for improvement

We recommend specific actions in the areas of assurance standards; testing and certification; cyber insurance; building sovereign capability; and securing government data.

Supplier assurance standards

There's a need for a single set of standards for the assessment of supplier security to be used across government procurement. Further work is needed to define exactly what this should be, but the key characteristics should include the following:

- Cover more than just technical IT controls by also including trust in the owners and employees of the supplier and a physical security component. The Defence Industry Security Program provides a good model for this, although required controls should be tailored to the level of risk.
- Go beyond a single pass/fail level by providing a number of graduated levels. This will allow buyers to tailor the minimum level they require based on the nature of the project, but also gives suppliers

a chance to show how they may exceed the minimum level, which may be considered an advantage in the evaluation process.

- Encourage independent certification to build credibility, combined with efforts to build the pool of available assessors, for example through ASD accrediting assessors and ongoing quality control through reviews of randomised samples of work.
- Ensure that, at the lower levels, it will be feasible for a large number of suppliers to be accredited in a short period of time. This will require ensuring that the criteria (for example, the existence of specific IT controls) can be readily evaluated.
- Ensure that, at the higher levels, the assurance criteria are based more on risk and outcomes, encouraging suppliers to take a mature approach and to put in place continuous ongoing improvement plans.

Where possible, we should aim to learn from and leverage the experience of other countries. While the Australian market and customers may have some specialised requirements, it should be carefully considered whether those requirements are worth the costs of diverging from a standard used by another major country. Apart from the direct costs and benefits of reusing something that works for one of our allies, export opportunities will be improved if local companies that are getting certified for the local market automatically have a certification recognised overseas.

One example to consider is the UK Cyber Essentials Scheme.[27] At the basic level, the scheme involves five basic controls that can be readily verified, and there's an enhanced 'Plus' level that also includes an independent security test of the company's systems. The UK Government has recently partnered with a commercial organisation to run the scheme and is reviewing the need for additional levels above and/or below those two levels.[28]

The US is getting ready to roll out CMMC (cybersecurity maturity model certification).[29] Although CMMC is specifically defence focused, it is aimed at 'controlled unclassified data', which can be a common requirement across all of government. It combines recommended practices from existing US federal procurement regulations, international standards and even ASD's 'Essential Eight', providing a graduated scale from level 1 with 17 specified practices through to level 5 with 10 times that number. It includes a requirement for independent certification even at the lowest level and is designed to scale across the whole US defence supplier base (more than 300,000 companies) using a phased transition plan. Guidance material is still being developed, but it generally mandates outcomes rather than specific technical controls, so vendors may need technical advice to implement it effectively.

Testing and certification processes

As noted above, assuring the security of a supplier and its systems is important, and that may be a sufficient safeguard when the potential risks concern sensitive data being handed over for processing or use by the supplier. However, where an IT product or service is being procured, supplier assurance in itself does not mean that the product or service is secure.

For hardware, particularly commodity hardware, customers may trust the vendor to do product assurance. This would require confirmation of the vendor's processes for assuring its own supply chains. For example, how does the supplier ensure the traceability of components and products,

verify chains of custody, and track any discovered vulnerabilities back to their point of origin? If there's concern over specific products having targeted backdoors for a given customer, the customer could insist on choosing the items themselves from general stock in a warehouse. As an additional safeguard against any interference in transit, delivery systems could have their entire software (including firmware, BIOS etc.) rebuilt from verified images provided by the manufacturer. Some government departments have well-established procedures for this, which could be shared across other departments and agencies to build capability and scale.

These approaches can work for 'commodity' hardware (products that are manufactured and sold in significant quantities globally) and where the manufacturer is trusted. A different approach is needed for more specialised systems, smaller or untrusted vendors, and particularly software, which is inherently more complex and susceptible to security vulnerabilities. Assurance may be from a combination of design assurance and testing of the delivered product.

ASD has run schemes to centrally evaluate and test commercial products and services, such as the Certified Cloud Services List (CCSL) and Certified Products List. However, those schemes have suffered from resource constraints, particularly the CCSL, which hasn't been updated for over a year. This has left government customers with the option of accepting self-certification from the vendor, with all the obvious risks and uncertainty that entails, or carrying out their own testing, which is likely to lead to, at best, duplication of effort among departments but more likely to the risk of inconsistent standards and potential failings due to the lack of specialist skills in each agency. A quick win would be to set up some sort of centralised library of evaluations carried out by individual departments, so that another department looking to use the same product could see and potentially reuse work already done.

Of course, care would be needed to ensure that a prior evaluation isn't reused without considering the relevance of the context. It would also be preferable if there were some independent oversight or review, such as by the ACSC, to apply a common standard across agencies to ensure that vendors can't 'game' the system by shopping around for the most favourable evaluation. This potential risk may be exacerbated by the recent decision for the ACSC to no longer maintain a list of certified cloud services and thus put the onus on individual departments. That announcement also suggested unspecified enhancements and uplift of the Information Security Registered Assessors Program. This could usefully include the suggestion that ASD accredits the certifiers and also provides some ongoing quality control through regular checking of a sample of the work undertaken.

However, ultimately, there needs to be an independent test and evaluation facility. If the ACSC doesn't have the resources or capabilities to run such a facility, it could seek a partner to implement it and provide some specialist staff to support and accredit the processes being used. AustCyber has proposed a 'sandbox' that could be used for general proving of capabilities to potential government clients.[30] Such a facility needs to be funded by the companies that are using it in order to ensure that it's appropriately resourced and used when it can add value. It's recognised that this could become a barrier to entry for small and medium-sized enterprises, but existing mechanisms (such as AustCyber's role in identifying companies with commercially viable propositions and in providing targeted grants) could address that problem.

The ACSC has announced plans to establish consultative forums with industry, the first of which focuses on cloud security.[31] The broader requirements for security testing and evaluation would be a suggested

topic for a subsequent forum. However, it's recommended that there be greater transparency about how industry representatives can be nominated and are selected—the announcement seems to suggest that the ACSC will select and invite representatives as it sees fit. When the Department of Home Affairs announced the establishment of an industry advisory panel for the 2020 Cyber Security Strategy, consisting of current or past executives of leading telecoms companies plus a representative of a US defence prime,[32] that appeared to lack diversity and, in particular, to exclude any representation of small and medium-sized businesses.

Mandatory cybersecurity insurance for suppliers

For all government procurements of IT products and services, suppliers should be mandated to have appropriate cybersecurity insurance cover, thereby ensuring that there's a price signal for risk. We've noted the problem that current mechanisms don't provide an incentive to spend more on better security. In other spheres, we see that insurance provides this incentive—those that behave in less risky ways and take steps to mitigate their risk are rewarded with lower premiums. For example, household insurers typically offer discounts for houses that are normally occupied during the day and have good locks and monitored alarm systems.

This would be similar to existing obligations for public liability insurance and in some cases professional indemnity insurance that are commonly found in government tender requirements. Insurance should cover incident response, resilience resources and third-party breach liability. Government customers often insert such obligations in contractual clauses, but this would provide assurance that the company can have access to the right people and has the financial resources to meet these commitments, irrespective of the size and nature of the business—thereby removing an implicit preference for larger established brands.

It's recognised that at present a number of factors are holding back the creation of an effective, functioning cybersecurity insurance market. Mandatory insurance would be a major factor in maturing the market, by ensuring sufficient demand to create economies of scale and building the overall volume of data that can be used for effective underwriting.

However, the market will require transitional support to manage the initial impact. Ideally, this move could be coordinated with Australia's allies to build global scale and critical mass, but it's unlikely to be practicable to achieve consensus without wasting the opportunity. If Australia is a global 'first mover' to make such a change, we'll need to ensure that this provides opportunities for local insurers while insulating local suppliers from any initial systemic shocks. Other countries will seek to learn from our experience, and we need to ensure that there's flexibility to also adapt in order to learn these lessons.

The supplier assurance scheme, with graduated levels of assessment, should be designed to also meet the needs of insurers to help them with assessing risk. Appropriate risk-weighted premiums will be vital to ensure that insurance doesn't effectively encourage risky behaviour or a false sense of comfort. The government may also need to regulate or even set up its own insurer to ensure that all companies have access to affordable cover in the short term. There's a precedent for this: the government established Medibank to keep the private health insurance providers honest, and when the market was working well was then able to privatise the company.

In the longer term, there may still be a need for the government to be a last-resort reinsurer for major nation-state attacks, in a role analogous to its role in terrorism incident reinsurance.

Building sovereign capability

We've seen that cybersecurity represents a great economic opportunity for Australian industry, and that supplier trust is important. This means that, especially for the most sensitive applications, the development of sovereign industry capability should be encouraged. The government should establish a sovereign capability framework, identifying which technologies it's strategically important to develop locally, and using that to guide more targeted mandated procurement and investment. An openly published framework would also help industry to prioritise its research and development to deliver in those areas. This would be analogous to the approach currently underway for the defence industry capability. This approach would effectively modify current procurement rules to allow government buyers to make decisions to prefer local suppliers where there's a compelling need for a sovereign capability.

The US has for many years gone much further under the Buy American Act, which mandates government to prefer local suppliers in all cases unless the price premium is more than 25%. Applying such a blunt approach in Australia would make government spending less efficient and risk conflicting with international trade agreements. However, at the very least, the government should ensure that there's a level playing field on which local companies of all sizes are able to have access to the market on an equal basis with global multinationals. There are arguments for a more measured 'Buy Australian' approach (for example, a target of, say, 5% of the IT spend on Australian companies) to be considered as a further step if sovereign capability development is slow to take off. This could act as a strong signal to those making procurement decisions about the importance of considering local suppliers.

Securing government data

Where sensitive government data is provided to suppliers, assurance that the confidentiality and integrity of that data will be protected is needed. There are numerous examples of breaches, such as fighter aircraft plans being stolen from a small defence contractor's network.[33] Also, even if no information is passed to the contractor, the data that the contractor generates and delivers (for example, detailed blueprints for designs that it produces under the contract) may be sensitive.

While there's a well-developed framework of security requirements for classified material, there can be significant risks involving unclassified but sensitive material that's generally less well protected.[34] We also see small businesses struggling to implement security on their IT systems to meet the requirements of the ISM with their limited budgets. While significant improvements can be made by improved basic cyber hygiene, for situations in which more sensitive data that may be of interest (for example, to nation-state attackers) is being processed, it's difficult to implement advanced monitoring and the required defence in depth.

To address this, the government should establish a secure cloud-based environment that contractors can use for projects under contract to the government. This would allow companies to process, use and generate data using suitable technologies to assure separation from the host systems of the supplier. The environment would need to be fully functioning and have the range of 'infrastructure as a service' and 'platform as a service' offerings that companies would need. In order to avoid the

overheads, and the moral hazard, of a government department trying to set up and run the assured environment, a better approach would be to license a small number of cloud vendors to provide it and to mandate suppliers to use one of those licensed services.

This approach should not only provide better assurance of data privacy and integrity but, by reducing the overheads of individual businesses implementing their own controls, should reduce the costs effectively charged by suppliers to government for compliance.

Conclusions

As the Australian Government looks to refresh its cybersecurity strategy in 2020, while end-user awareness and education will be important, the onus needs to be on the government and the private sector to uplift security across the board and make the lives of adversaries in cyberspace more difficult. Government has limited human and financial resources and so needs to use them as effectively as possible. The significant overall ICT procurement spend by government represents an opportunity to do so, but is currently hampered by a fragmented approach, differing standards and regulations, and procurement approaches that don't facilitate value being attached to innovative security approaches and sovereign capability.

Our main policy recommendations to address these challenges are as follows:

- The Australian Government, working with the state and territory governments, should include in government procurement strategies consideration of how governments can use their market power to encourage better cybersecurity in what they purchase, and use that approach to encourage suppliers to improve the security of their offerings in all customer sectors.
- Simplify the current array of supplier standards to a single set that provides multiple levels that can be used for different risk levels and also allow suppliers to demonstrate progress and enhanced levels of security.
- Address gaps in the market for independent testing and certification, allowing buyers to be confident about the security of products and services and companies to be able to demonstrate and prove innovative approaches.
- Follow up the recent announcements on the future of the CCSL and Information Security Registered Assessors Program by establishing a framework to standardise and assure the quality of work of independent assessors to provide a viable alternative, and ensure that industry consultations on future requirements are fully inclusive.
- Ensure that risks to security are effectively factored into supplier quotes by investigating how a mandatory insurance regime could operate.
- Develop and implement a sovereign capability strategy to ensure market opportunities for Australian companies of all types and sizes in order to build local capability in the most sensitive areas and to exploit the global economic opportunity that the cybersecurity market provides for local industry.
- Use shared services approaches to ensure that consistent best practice is applied for the secure handling of sensitive data by government suppliers, without duplication of cost and effort.

Appendix: Detailed review of tender documents

Department / agency	ATM-ID	Title	PSPF	ISM	Specific supply-chain requirements	Other standards mentioned	Other requirements
Great Barrier Reef Marine Park Authority	ATM000039	Application development services	N	N	N	–	Provide integrated security with authentication and authorisation
Digital Transform-ation Agency	DTA–487 V2	Digital Marketplace Panel	N	N	N	–	Cybersecurity is one category for which proposals are sought
Airservices Australia	ATM19–00007	ADS-B Expansion Project	(Indirect)	Y	N	ISO 27001	Additional cyber requirements, including data handling, software code reviews, testing, 'reasonable efforts' to prevent harmful code
Reserve Bank of Australia	RBA. IT.2020.01	Cisco Data Centre Compute	Y	Y	N	–	Other requirements, including control of customer data, software to have 'strongly identifiable security properties and peer reviews'
Department of Education	RFT PRN 2–19–2	Develop and roll out online teaching and learning resources in mathematics and numeracy	Y	Y[a]	N	ASD mitigation strategies, AS 31000	Detailed requirements, including calling out specific ISM sections, patching requirements etc.
National Capital Authority	NCA C19/234	Managed ICT services	Y	Y	N	NIST–800, ISO 27001, ASD crypto evaluation, ASD mitigation strategies	Specified controls, including logging, patching, broad requirements for protection of data, and a requirement to use 'best available security controls and features'
Reserve Bank of Australia	RBA. IT.2019.09	Server patching and software deployment capability or service	–	Y	N	NIST, ISO 270001	Eight requirements for specific controls, plus requirement to provide details of information security management system
Office of Parliamentary Counsel	OPC/1920–01	Provision of cloud hosting and other related services	–	Y	Y	–	Authentication and access control, security management plan and reporting
CSIRO	CSIRORFT 2019045	Pawsey Super-computing System	Y	Y	Y	–	Several pages of detailed requirements

Department / agency	ATM ID	Title	PSPF	ISM	Specific supply-chain requirements	Other standards mentioned	Other requirements
Australian Tax Office	SPC–2896–1	Managed network services— network manager, unified communications and contact centres	Y[b]	Y	Y	–	Specific controls and prohibitions, detailed as relevant to the technical specifications
Digital Transform-ation Agency	DTA-ICT–098	Telecommun-ications marketplace	Y	Y	Y	–	'Security measures no less rigorous than accepted industry standards'; supply-chain requirements; potential hook for mandatory cyber insurance; general requirements for access control, logging etc. 'in accordance with Buyer instructions and policies'

ISM = *Information security manual*; PSPF = Protective Security Policy Framework.
a Multiple overlapping requirements in different places. In one place requires complete compliance with ISM; in another only refers to 'relevant parts of', then calls out specific parts of the ISM as separate compliance requirements.
b Requires 'consistency with' PSPF and ISM, rather than compliance.

A further six tenders were Defence related. They're listed separately below as they have specific Defence-related approaches.

Department—group	ATM ID	Title	Requirements
Department of Defence—DSRG	Cyber Call 2019	Next Generation Technologies Fund—CYBER Broad Area call for proposals	Detailed requirements for cybersecurity-related projects
Department of Defence—CASG	JSD/IB/12089/1	Enhanced Geospatial Support System	Detailed Defence-related requirements
Department of Defence—CASG	JSD/RFT/7146/1	Enhanced Defence High Frequency Communications System	Detailed Defence-related requirements
Department of Defence—DSRG	11870	WHS Hazardous Chemicals Register	Pre-release notice only, but notes requirement for Australian-based solutions
Department of Defence—DSRG	HUB–16-PIN-SIF–001g	Defence Innovation Hub—call for submissions	Refers to CDIC site for detailed requirements
Department of Defence—CASG	JSD/NOT/12477/1	Joint Project (JP) 9102 Australian Defence Satellite Communications System	Detailed Defence-related requirements

Notes

1 Rob van der Meulen, 'Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016', *Gartner*, 7 February 2017, online.

2 Australian Signals Directorate (ASD), *Annual report 2018–19*, Australian Government, 2019, online.

3 ASD, Australian Cyber Security Centre (ACSC), *Cybercrime in Australia: July to September 2019*, Australian Government, no date, online.

4 Henry Belot, 'Federal government's $10b IT bill now rivalling Newstart Allowance welfare spend', *ABC News*, 28 August 2017, online.

5 Justin Hendry, 'NSW govt IT spending tops $3bn', *ITNews*, 1 August 2018, online.

6 Digital Transformation Agency (DTA), *Whole-of-government hosting strategy*, Australian Government, no date, online.

7 Australian Building and Construction Commission, *What is the code?*, Australian Government, no date, online.

8 Department of Finance, *Commonwealth Procurement Rules 20 April 2019: achieving value for money*, Australian Government, 2019, online.

9 DTA, *Buying digital products and services for government*, Australian Government, no date, online.

10 HP Inc., *IDC Government Procurement Device Security Index 2018: Public sector PC & printer RfPs lack basic security consideration*, IDG Connect, 21 March 2019, online.

11 Attorney-General's Department, *Protective Security Policy Framework*, Australian Government, no date, online.

12 ASD, *Australian Government information security manual*, Australian Government, January 2020, online.

13 ASD, *Essential eight security model*, Australian Government, July 2019, online.

14 ASD, *Strategies to mitigate cyber intrusions*, Australian Government, February 2017, online.

15 International Organization for Standardization, *ISO/IEC 27000: Information technology—Security techniques—Information security management systems—Overview and vocabulary*, 5th edition, February 2018, online.

16 PCI Security Standards Council, *Document library*, no date, online.

17 AusTender, online.

18 DTA, *About the Digital Service Standard*, Australian Government, no date, online.

19 See, for example, Australian National Audit Office, *Cyber resilience*, performance audit report no. 53 of 2017–18, 28 June 2018, online.

20 ASD, ACSC, *Small business cyber security guide*, Australian Government, October 2019, online.

21 ASD, ACSC, 'Joint Australian Signals Directorate and Digital Transformation Agency public statement on independent review of CSCP and IRAP', news release, March 2020, online.

22 ASD, ACSC, 'Joint Australian Signals Directorate and Digital Transformation Agency public statement on independent review of CSCP and IRAP'.

23 'Publications', *Common Criteria*, no date, online.

24 AustCyber (Australian Cyber Security Growth Network), *Australia's Cyber Security Sector Competitiveness Plan 2019: Driving growth and global competitiveness*, 2019, online.

25 Kitty Ho, *The state of the cyber insurance market*, Actuaries Digital, 7 November 2019, online.

26 Brian Corcoran, 'What Mondelez v. Zurich may reveal about cyber insurance in the age of digital conflict', *Lawfare*, 8 March 2019, online.

27 National Cyber Security Centre, 'Protect your organisation against cyber attack', *Cyber Essentials*, UK Government, no date, online.

28 National Cyber Security Centre, 'The bare essentials', *Cyber Essentials*, UK Government, 22 June 2019, online.

29 Carnegie Mellon University, Johns Hopkins University Applied Physics Laboratory LLC, *Cybersecurity maturity model certification (CMMC)*, version 1.0, 30 January 2020, online.

30 AustCyber (Australian Cyber Security Growth Network), *Submission: 2020 Cyber Security Strategy consultation*, November 2019, online.

31 ASD, ACSC, 'Joint Australian Signals Directorate and Digital Transformation Agency public statement on independent review of CSCP and IRAP'.

32 Rohan Pearce, 'Telstra CEO to lead industry panel for government's cyber strategy', *Computer World*, 26 November 2019, online.

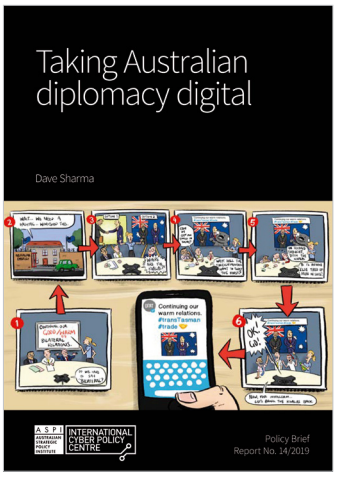
33 Stilgherrian, 'Secret F-35, P-8, C-130 data stolen in Australian defence contractor hack', *ZDNet*, 11 October 2017, online.

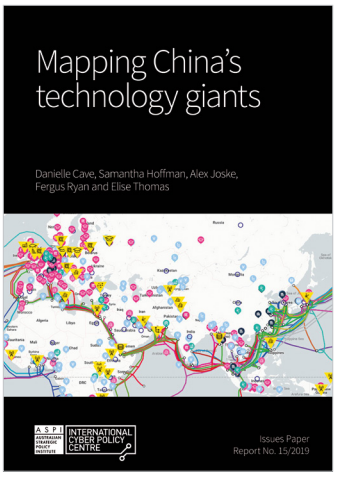
34 See, for example, Anna Henderson, Andrew Greene, 'Fears private details of defence force members compromised in database hack', *ABC News*, 4 March 2020, online.

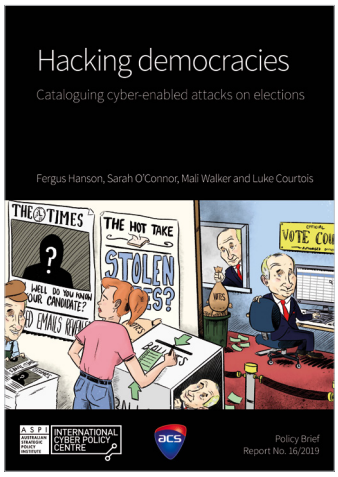
Acronyms and abbreviations

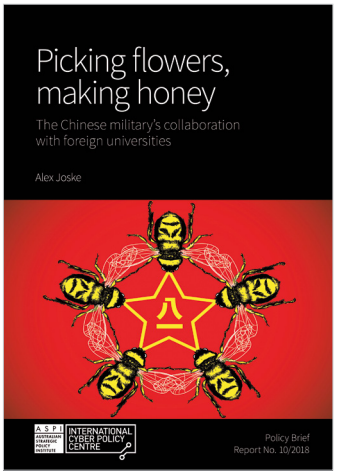
ACSC	Australian Cyber Security Centre
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CCSL	Certified Cloud Services List
CMMC	cybersecurity maturity model certification
DTA	Digital Transformation Agency
ICT	information and communication technology
ISM	Information security manual
IT	information technology
PSPF	Protective Security Policy Framework

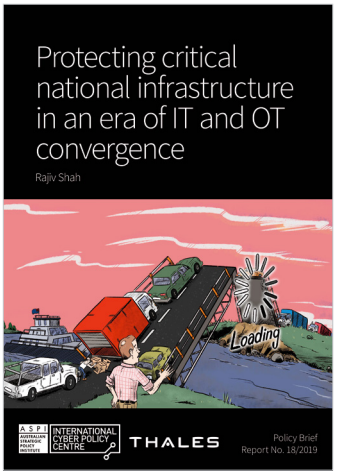
Some previous ICPC publications

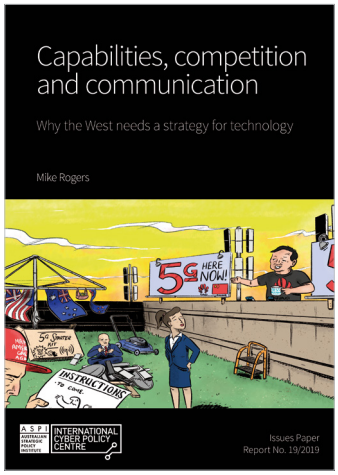


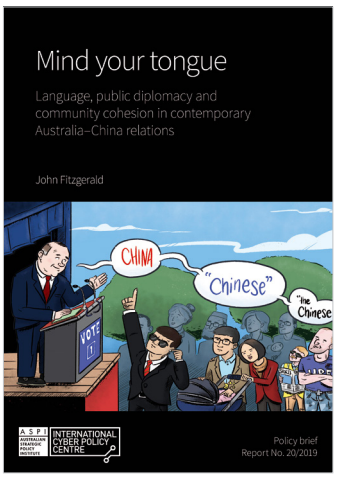












ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

macquarie
GOVERNMENT