National Institute of Strategic Resilience
ABN 60 645 040 231
Level 1, The Realm, 18 National Circuit Barton ACT 2600
P: +61 2 6198 3256 E: info@nisr.org.au W: www.nisr.org.au

2023-2030 Australian Cyber Security Strategy Discussion Paper Response

On behalf of the National Institute of Strategic Resilience

About Us:

The National Institute of Strategic Resilience (NISR) is an emerging independent research and delivery organisation, dedicated to enhancing the resilience of nations and the cohesion of societies. Our mission is to promote a comprehensive and integrated approach to resilience that encompasses all aspects of society and the supporting systems of state.

At the core of our work is the NISR Resilience Framework, a tool for scoping the complex interdependencies between different domains of resilience, value chains, and societal optics. This framework supports six domains of resilience, including sovereign and democratic resilience, infrastructure and service resilience, supply-chain resilience, digital and cyber resilience, economic resilience, and environment and climate resilience.

As a research organisation, NISR draws on a range of expertise from academia, industry, and government to develop innovative solutions to enhance national resilience. Our networked team of experts includes specialists in cyber security, risk management, critical infrastructure protection, and environmental sustainability, among others.

NISR's vision is to help build a safer and more secure world by enhancing national resilience. We believe that resilience is not just about bouncing back from crises, but about building the capacity to adapt and grow in the face of adversity. By promoting adaptation and growth, we are talking about resilience in a strategic context, hence we define the term ‘strategic resilience’.

The NISR submission to the 2023-2030 Cyber Strategy is based on the foundational belief in a whole of society approach to security and privacy. We have placed particular emphasis on support for the less resourced areas of our society, such as small businesses and vulnerable citizens. We recognise that these are the sectors where profit driven organisations may not choose to focus their investments, and representation is likely needed by peak bodies and not-for profit organisations.

Response to Questions

Before addressing individual questions, we would make three points.

First, **cybersecurity is a subset of strategic resilience more broadly**. It makes little sense to consider cyber resilience without placement in the broader context of society, the economy and national purpose.

Accordingly, it makes better sense to focus on individuals and communities, rather than state institutions, as building blocks for national resilience. Local knowledge is key, and locals—individuals, teams, small businesses, and communities—need agency (including their own definitions of safety), knowledge, and support.

At the level of organisations, the ability to anticipate—not predict—and then contain the inevitable failure, is key. Again, this requires local knowledge and typically deep expertise.

At the national level, government would do well to learn from and adopt a complex systems approach. We know from the pandemic, and from Ukraine's hardening of its systems after 2014, the importance of redundancy, buffering, modernisation, skills, and practice.

All have costs, which will need to be met, as in a disrupted environment, the alternative may be worse. That will mean to be taken seriously, a new strategy will need to have a clear allocation of resources—and budgets are where the rubber hits the road.

Second, addressing strategic resilience in the context of cybersecurity must be **contextual, adaptable and allow for graceful failure**. And there will be flaws and failure; it's the nature of exceptionally complex and constantly evolving fungible software systems.

But thus far, while democracies are susceptible to micro-failures they are proving macro-resilient. Those are attributes we want to encourage; we want to avoid reforms that introduce brittleness and rigidity, that hamper adaptability, that dampen energy, and that dissuade innovation, contestability, and open and forthright discussion.

Further, because we are a democracy, we need to ensure provision of recompense and care for the affected. Too often victims are blamed, which impedes the sharing of experience and learning from each other. And too often risk is transferred to those least able to bear it.

Third, **cyber is corrosive**: it is both ubiquitous and deep, affecting all layers of society, systems, and human activity.

Cyber is not simply a disruptive tool in the hands of criminal elements, but also a means of nation-states, including the Australian government, exerting power and influence. Critically, because anything digital has an inherent cyber characteristic, and digital technologies are now deeply embedded in our everyday lives, cyber is integral to the immediate wellbeing of individuals and their personal freedoms.

Balancing the challenges posed by preventing the activities of multiple sets of actors while seeking to enable freedom of state action, the wellsprings of economic activity, and retain democratic legitimacy is no simple task. Trust is critical to government effectiveness—but that trust must be earned.

That, perhaps counterintuitively, lessens its ready reducibility to legislative remedies. Governments cannot know everything about the system—or even enough to act with certainty. It's tempting to over-reach, to demand certainty and seek to coerce outcomes—or, at the other end of the spectrum, simply abandon citizens and companies and expect them to cope. And in the process, lose trust and legitimacy.

Cyber is a new strategic domain; others may yet emerge through further technological developments. How it is handled has immediate implications not simply in terms of geostrategic competition, or our economic wellbeing, but for the nature of our democracy.

Addressing these issues will not be resolved in this single document. What we are looking for is a path for ongoing and meaningful debate; a commitment to keeping the aperture of opportunity and contestability open, and a means to enable that engagement.

Last, we note that the consultation and process of submission can demand a substantial investment of time, resources, and expertise, which may not be readily available to smaller organisations. The risk is that the voices of this sector will be diminished by the larger incumbents. It is imperative that we take steps to level the playing field and keep the aperture of opportunity and contestability open. NISR will draw on its own experience and position as a start-up and small not-for-profit business to contribute to this process. Addressing these challenges will not be resolved in this single document, but it is a path to enable that engagement.

Question 1.

What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

Given the pace of technological, geopolitical, and social change, it will be difficult to craft a strategy that is fit for the world of 2030—a full seven years hence. A more robust approach may be to prototype a series of principles, supported by a series of initiatives, that support resilience. They may include the following.

Strengthen democratic norms and systems. This is a key expression of purpose and culture at the national level, and targets institutions. Initiatives may include, for example, bolstering individual privacy protections, enforcing agency accountability and reporting, and establishing a cyber ombudsman.

Further, we suggest establishing an ongoing, structured open forum with organisations and the community about the nature of digital democracy—capturing both opportunities as well as the challenges, ie including cyber. These are matters that cannot be resolved within the government's

typical consultation period of three months. Rather, a lesson may be drawn from various European models, where all elements of society are engaged in open, structured discussions, and research and ideas drawn from and tested by more than outsourced consultants, over some years.

Local knowledge matters. Government has unique capabilities and responsibilities. But it is also in the nature of much software—especially outside commodity platforms such as corporate, ERP systems and core networks—that its application and evolution in real world conditions can become highly tailored and bespoke, and that organisations will use different systems in different ways. Further, data is highly contextual—and can be exceptionally personal, integral to the core identity of individuals.

It makes sense to harness local knowledge as much as possible. That suggests that to help companies, especially the SME sector and individuals, anticipate and prepare for cyber, the government may consider a variation of the extension officer scheme, similar to that which helped build Australia's agricultural sector, as well as a social fund for skills, protection, tool building and events for community organisations, and supporting organisations such as NISR for research, contestability and debate.

Find and partner with like-minded friends. The cyber environment is vast, highly opportunistic, and constantly changing. Australia is engaged in a competition for attention, goodwill, knowhow, and skills. In such an environment, our friends are not simply other nation-state governments, or groupings such as the Five Eyes community or AUKUS—they may include dissidents in authoritarian regimes.

Because the cyber environment operates at physical, logical and human and cognitive levels, having as many touch points as possible and means of understanding the nature of threats is important—especially as they impinge with grey zone activities. The government could consider a hybrid threat centre as per the Hybrid CoE. Having a trusted space guaranteed by inalienable, legally guaranteed rights to security, integrity and privacy, would help build confidence in a region already under pressure from aggressive grey zone activities, including cyber.

Trusted government (systems and data). The government contains vast amounts of data on Australian citizens and businesses—and as the Robodebt Royal Commission has shown, even simple manipulation of that data can have devastating effects on individuals, and on trust in government and its systems. The security and protection of both data and systems are essential to forestall loss of confidence and trust.

It is also one area where government has most control i.e. its own systems—and where it has yet to meet its own standards. And it is one area, too, that it cannot simply hide away from scrutiny—indeed, red teaming, testing by outsiders, and contestability are essential if government is to ensure its systems are sufficiently hardened and its actions are trusted.

Ongoing learning/learning never ends. Learning, both knowledge and practice in all areas of technology, cannot stop. Moreover, cyber skills are already and have long been short, and the pressures for graduates in cyber is increasing with pressure from other critical areas in the economy and national priorities, from medicine to nuclear physics and engineering to quantum computation, to

ICT skills of all kinds, to AI and robotics, etc, as well as the standbys of mining, agriculture, broader health professions and financial services.

In short, there is no ready solution, and no university course ready to resolve the issue. Instead, new modes and new pathways need to be investigated, regulation may need to be eased, and lifelong learning, including an allocation of 20 per cent of time dedicated to education. Further, current university fees and means of delivery are a barrier to later learners, or people looking to change careers, and should be rethought.

Technology—not just cyber—skills. Cyber is a mix of human, social, political, legal, physical, financial, and technological drivers and outcomes. It may be a better outcome to educate and season 1000 'technologists', who can understand the implications and know what questions to ask, than focussing only on a small, highly specialised, group of staff.

Not just STEM. Often it is mindset, not underlying technological skills, for which those critical cyber teams recruit—and those mindsets may be found in people of all walks of life. Further, whereas STEM is key to understanding the 'what' and the 'how', the humanities are central to understanding the 'why', and the people side of the equation. Both are critical to building broader resilience.

Leadership matters. Cybersecurity leadership is currently based on individual best effort. Done well, cybersecurity offers a huge source of competitive advantage for businesses, and of trust and integrity for government. And it's essential to building the bridges and practice between government, industry, and the not-for-profit sector. But all are falling short, too often because the systems, support, and professionalisation that helps bring the best talent to the table, and helps build the conditions for success, are missing.

That said, design suitable for today is also likely to fall short. For all that, the seven years intended for this strategy is a hard call. People take time to learn, develop and be seasoned. We need to think ahead for the likely skills sets and professional development path needed for this group of cross-domain technological leaders. In the meantime, the government would do well to deliberately encourage and recruit diverse and disruptive thinkers and practical doers into its policy and operational midst.

Other questions.

Many of the other questions contained within the consultation paper are subsidiary to the more fundamental principles and initiatives above. Some lie outside our immediate focus. However, we share some further, question specific, considerations in Appendix A.

Contacts and Feedback

NISR supports efforts by government, industry, and the community to improve Australian cybersecurity and cyber resilience. Making Australia the most cyber secure democracy, let alone nation, in the world by 2030 is an exceptionally tough ask—but a suitably ambitious goal.

Most recently, we have been focussing on the protection of vulnerable citizens from the effects of cybercrime; related policy proposals emerging as part of a National Strategy would be of immediate

interest. More generally, however, our purpose remains centred on the concept of strategic national resilience, and we look forward to engaging with the Department of Home Affairs and its fellow departments to that end.

Co-authored with contributions from the NISR advisory council.

For further information contact:

Alison Howe
Chief Executive Officer

National Institute of Strategic Resilience
L1, The Realm
18 National Circuit,
Barton, ACT 2600.
Australia

M: +61 02 6198 3256
E: policy@nisr.org.au
W: nisr.org.au

ABN: 60645040231
An ACNC Registered Charity

Appendix A – Further reponses

The following body of work provides individual responses to elements of the discussion paper for consderation by the panel. These reponses are subordinate to the themes addressed in our response to Question One and therefore presented as an Appendix.

Responding to Question 2 & 19:

> *Question 2: What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy; cyber secure nation in the world by 2030?*
>
> Question 19: *How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?*

Cyber Security Regulations for Internet-Connected Devices

NISR recognises the increasing threat posed by Internet-connected devices or IoTs, and believes that the government should take legislative or regulatory actions to enhance cyber resilience across the digital economy.

IoT devices are often an overlooked and unsecured attack surface, and incidents such as the 2017 North American casino hack and the 2020 Australian security camera hack illustrate the risks posed by these devices. The government should use its unique capability as a market and product regulator to address these risks, and consider:

- Minimum cyber security requirements on IoT and internet-connected devices (such as unique default credentials), and/or
- Cyber security ratings on internet-connected devices; similar to energy and water star ratings, which would enable consumers to make informed decisions about the security of the devices they purchase.

Implementing minimum cyber security requirements and/or cyber security ratings for these devices would promote security by design in emerging technologies and enhance cyber resilience across the digital economy.

Responding to Question 2c

Question 2c: *Should the obligations of company directors specifically address cyber security risks and consequences?*

Cyber Security Requirements for Company Directors

NISR recognises the importance of cyber security governance and compliance for critical infrastructure providers. We support the new requirement outlined in Section 30AG of the SOCI Act for the board or governing body of these providers to submit an annual report to Home Affairs, attesting to their compliance with cyber security requirements.

This new requirement places accountability for cyber security governance and compliance squarely onto the board, which is an important step towards ensuring that cyber security is taken seriously at the highest levels of these organisations. However, given that the s30AG requirement has not yet come into effect, the government should take this opportunity to track and assess forthcoming adoption of the requirement to determine its impact on cyber resilience.

The government could engage an independent third party to assess the effectiveness of the s30AG implementation, and to determine whether board members are effectively interpreting their responsibilities. This will help to ensure that the new requirement is achieving its intended outcomes and will enable the government to identify areas for improvement.

Based on the outcomes of the s30AG implementation, the government may consider implementing a similar cyber security attestation requirement for other groups of company directors. This would promote cyber security governance and compliance across a wider range of organisations and industries and help to ensure that cyber security is taken seriously at all levels of these organisations.

Responding to Question 2f & 9

Question 2f: *Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:*

a. victims of cybercrime; and/or

b. insurers? If so, under what circumstances? and

Question 9: *Would expanding the existing regime for notification of cyber security incidents (e.g., to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?*

Ransomware Payments

NISR recognises the complex nature of ransomware payments and believes that the government should carefully consider the circumstances under which the payment of ransoms should be allowed.

While the payment of ransoms directly funds criminal organisations and encourages future ransomware attacks, there may be certain situations where organisations need the flexibility to pay a ransom. For example, if a hospital or critical electricity provider were attacked, the negative impact on society may outweigh the negative impact of paying a ransom. Therefore, a complete ban on ransom payments may not be practical or effective.

However, the government should discourage the payment of ransoms and encourage organisations to adopt proactive measures to prevent and mitigate ransomware attacks. The Australian Federal Police have recommended that individuals and organisations should not contribute to the ransomware crisis by paying ransoms.

The government should consider reintroducing the Ransomware Payments Bill that lapsed at the end of the last Parliamentary cycle. The Ransomware Payments Bill would require organisations and/or their insurers, that seek to pay a ransom, to notify the Australian Cyber Security Centre (ACSC) of the details of the attack and of the payment. This would provide the government with more accurate information on the trend of ransomware and of important details of ransomware attacks.

If the government were to prohibit ransom payments, it may drive the practice underground and disincentivize organisations from engaging with the government in the event of a ransomware attack. Instead, the government should consider mandatory reporting of ransomware or extortion demands under the existing regime for notification of cyber security incidents. This would improve public understanding of the nature and scale of ransomware and extortion as a cybercrime type and enable the government to respond more effectively to these incidents.

Responding to Question 8 & 13

Question 8: *During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?* And

Question 13: *How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?*
Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

The Government's Cyber Incident Response Procedures

NISR recognises the importance of government support in response to a cyber security incident, and the need for clarity on the roles and responsibilities of all stakeholders.

While the government can provide some support to organisations in the event of a cyber security incident, this capability should be predominantly provided by private sector actors. The government should review its cyber security incident response support engagement procedures to ensure clarity for all stakeholders on the role and expectations of the federal government in responding to cyber security incidents outside federal government networks.

To improve engagement with organisations that experience a cyber incident, the government should consider the following:

- **Confidentiality**:
  Explicitly stating that private personal information should not be provided to the government during an investigation is particularly important given that organisations are not subject to the Office of the Australian Information Commissioner's (OAIC) Privacy Principles when exposing employee data. The government should demonstrate best practice to industry by codifying the process of securing and/or destroying victim artefacts after an investigation.

- **Indemnity from self-incrimination though reporting**:
  Victims of cyber crime should be protected from self-incrimination by the act of reporting. Information obtained as part of a cyber crime report and/or during a cyber security incident investigation should not be used to undertake regulatory or civil action against the victim organisation. Protection from self-incrimination should not extend to serious criminal matters.

  The Director General of the Australian Signals Directorate (ASD), Rachel Noble has previously defended the concept of a 'safe harbour' provision for organisations when reporting cyber attacks.

- **Centralisation of reporting requirements**:
  Victims of cyber crime should be able to report to the ACSC and have that report shared with relevant regulators. This would support information-sharing between government entities and reduce the burden on victims.

- **Threat sharing**:
  The ACSC should ingest cyber incident reports and use deidentified information from those reports to produce threat intelligence products/alerts for government and industry.

To clarify the government's role in the context of other actors, the government should work with various stakeholders such as law enforcement, banks, insurers, and telecommunications service providers to develop clear norms on the roles and responsibilities of various stakeholders prior to, during, and following a cyber attack.

Clear expectations will allow stakeholders to focus on their responsibilities and develop advanced capabilities required to fulfil their role.

Responding to Question 10

Responding to Question 10: *What best practice models are available for automated threat-blocking at scale?*

Active Cyber Defence

NISR recommends that the government work with industry stakeholders to identify efficient and scalable mechanisms to reduce the effectiveness and/or raise the cost of commodity-scale cyber attacks.

The UK's Active Cyber Defence (ACD) program, operated by the National Cyber Security Centre (NCSC), and Telstra's Cleaner Pipes initiative, are both good examples of scalable and automated interventions that can be considered.

The UK NCSC's ACD program is designed to harden the UK against high volume, low complexity cyber attacks through a suite of automated interventions, including a takedown service, mail check, web check, and protective Domain Name System (DNS) blocking. In its first year of operation, the ACD program was able to assist in halving the UK's share of global phishing attacks, taking down almost 140,000 UK-hosted phishing sites.

Domestically, Telstra's Cleaner Pipes initiative attempts to block malicious content before it reaches the end user. This initiative has been successful in blocking millions of scam calls, texts, and emails per month, demonstrating the effectiveness of simple, scalable technology in responding to commodity-scale cyber attacks.

By adopting best practice models such as the ACD program and Cleaner Pipes initiative, the government can work towards reducing the effectiveness of commodity-scale cyber attacks, and improve Australia's cyber resilience.

Responding to Question 15

Responding to Question 15: *How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?*

An accountability framework for victims of cybercrime

NISR seeks to highlight the issues faced by victims of cyber crime, particularly those who are elderly or otherwise increasingly vulnerable. (Reference our recent article in the Canberra Times)

We are calling for the creation of a clear accountability framework to help establish 'who does what' when a citizen is bereft of their data, identity, or their savings. The issue was highlighted by Jon Faine in his recent article in the Sydney Morning Herald:

"John notified his bank, which said it could do nothing. He asked banking watchdog Australian Prudential Regulation Authority to intervene. APRA referred him to the telecommunications watchdog, the Australia Communications and Media Authority, as a telco ought to be responsible for the carriage of a fraudulent text message.

AMCA referred his complaint back to APRA, which next sent his email to the Australian Financial Complaints Authority (AFCA), which in turn recommended he take it up with his bank".

There is a clear need for citizens to know where to go for help, and 'who is accountable for doing what' in their times of dire need.

NISR proposes that there should be an International Accountability Framework but suggests that establishing such a framework in Australia would be a useful start.

Responding to Question 15a

Question 15a: *What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?*

Small Business uplift at scale – beginning with those covered by the Privacy & SOCI Acts

The issue of small business cyber security is a well-documented 'wicked problem'. The co-founders of the National Institute of Strategic Resilience have published on this subject over the past four years, without seeing any positive change in the risk posture of the sector.

NISR believes that government assistance is needed to break the deadlock that exists at the convergence of poor resources, limited 'know how', limited time, and limited interest in the face of day-to-day business management. We advocate that government should prioritise small businesses

that deal with data that falls under the Privacy and/or SOCI Acts. These businesses would benefit from a mix of incentive, mandate and support to tackle a cyber resilience uplift.

Small businesses are a vital component of the Australian economy, accounting for more than one-third of industry value added (IVA) and 33.2% of GDP in 2020 (ABS, 2021). Initiatives to create 'at scale' cyber uplift in this sector have been tried, and mostly failed, over the years. Therefore, we advocate that government focuses on a trial segment of the small business community to test a scalable approach. We propose that government looks to the small businesses suppliers of the National Disability Insurance Scheme (NDIS), which provide support for people with disabilities in Australia. These suppliers often handle sensitive client data, making them a prime target for cybercriminals.

Addressing small business cybersecurity in these areas should be a priority for the Australian government, particularly given the vulnerable nature of the clients being supported by the NDIS. According to the NDIS Quality and Safeguards Commission, there were over 430,000 Australians receiving support through the NDIS as of June 2021 (NDIS, 2021). These clients may have complex support needs and may require sensitive health and personal information to be shared with NDIS suppliers.

If small businesses that supply services to the NDIS are unable to adequately protect sensitive client data, it could have serious consequences for the privacy and safety of vulnerable individuals. Cyber attacks on NDIS suppliers could also disrupt the provision of essential services and support for people with disabilities.

Therefore, the Australian government should prioritize the cybersecurity of small businesses in areas servicing vulnerable citizens or otherwise covered by the Privacy Act. We suggest a mix of incentives, mandate and support should be provided to help them improve their cybersecurity posture. This could include targeted education and training programs, access to cybersecurity tools and managed services, and financial assistance to help businesses implement stronger security measures. Ideally, a simple, low cost managed service for small businesses on a per-end point basis.

Our experience suggests that whilst cyber training and education are important for small business owners, they are often not prioritised. Education should preferably focus on obligations to meeting the provisions of the Privacy Act, rather than broader cyber security training initiatives at the outset.

By protecting the cybersecurity of small businesses that supply services to vulnerable Australians, the government can help to safeguard the privacy and safety of these citizens whilst demonstrating a pathway for other small business segments.

Responding to Question 16 & 18

Question 16*: What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?* And;

Question 18: *Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?*

Supporting the Uptake of Secure Technologies

Expanding the use of MyGovID or other identity management technologies

The collection and storage of personal data is a growing concern for Australians, as data breaches and identity theft continue to make headlines. To address this issue, the government should explore solutions for citizen identity management.

Concern around the use and storage of Australian's personal data has increased over the last 12 months in response to significant data thefts at Optus, Medibank, and Latitude Financial.
Given the growing public concern around the collection and storage of personal identity documents, and the inability to opt out of many of these, the government has grounds to propose a scalable solution to protect all Australians.

One such solution could be the development of a decentralized identity management system that enables citizens to control their own data and share it only with authorized parties. Decentralized identity solutions offer a secure approach to identity management that puts individuals in control of their own data.

Alternatively, government could investigate the viability of the MyGovID platform to be made available to the private sector. The government could provide this as a paid service, therefore reducing the cost burden on the government. However, we acknowledge potential issues regarding a government-controlled identity platform and the digital rights lobby.

Ultimately, the government should prioritize the development of a comprehensive identity management strategy that is built on ethical principles and potentially, open-source technologies. By doing so, the government can ensure that all Australians have equal access to secure identity storage and that their personal data is protected from cyber threats and identity theft.

Responding to Question 18

> Question 18: *Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?*

Leveraging Supply Chains and Procurement to Support National Cyber Security

Leveraging supply chains and procurement is an important aspect of national cyber security. Section 93 of the Public Governance, Performance and Accountability Act provides the finance minister with the power to require a government business entity to implement a government policy order. This power has already been used to support good cyber security by enforcing the Protective Security Policy Framework (PSPF) for non-corporate Commonwealth entities.

To further strengthen cyber security, the finance minister should consider using their power to require large non-corporate Commonwealth entities to abide by the same supply chain security requirements as critical infrastructure entities regulated by the Security of Critical Infrastructure Act. This

requirement should be limited to entities that have the means to effectively implement these requirements.

By extending these requirements to non-corporate Commonwealth entities, the government can help to ensure that cyber security is considered throughout the supply chain and procurement process. This would include implementing security measures for suppliers, conducting risk assessments for suppliers, and ensuring that suppliers are compliant with cyber security regulations.

The government should work closely with industry to develop guidelines and best practices for supply chain and procurement cyber security, and to ensure that these requirements are practical and achievable for large non-corporate Commonwealth entities.

Overall, leveraging supply chains and procurement to support national cyber security is a crucial step in protecting critical infrastructure and securing sensitive data. The government should use its powers under the Public Governance, Performance and Accountability Act to ensure that large non-corporate Commonwealth entities are subject to appropriate cyber security requirements, and work with industry to develop guidelines and best practices for supply chain and procurement cyber security.

Recommendations not Mapped to Questions

Civilian Cyber Corps

Australia simply does not have sufficient cyber security professionals to ensure the economic and national security of our internet-connected society. In 2019, AustCyber, the Australian Cyber Security Growth Network, predicted that Australia would face a shortfall of 17, 000 cyber security professionals by 2026. This year, think tank Per Capita, in conjunction with CyberCX, predicted a shortfall of 25-30, 000 professionals across the broader ICT sector by 2024; suggesting that it is not an issue that can be addressed by simply upskilling ICT professionals in cyber security.

These human resources shortfall cannot be fixed through immigration alone. The recent $(ICS)^2$ 2022 Cybersecurity Workforce Study identified a global cyber security professional shortage of 3.4 million. While Australia has traditionally been able to mitigate some skills shortages through immigration, the global shortage and international competition will make this more difficult. Further, many cyber security positions, especially those in government roles, require security clearances that are difficult for foreign-born Australians to attain.

The cyber security professional shortage is even more acute for government entities. Compared to the private sector, Australian and state government cyber security professionals will often have:

- Lower average pay.
- A need to manage people as part of their career progression, rather than simply increasing their technical mastery.
- Other requirements such as physical or uniform requirements.

The Government should consider establishing a Civilian Cyber Corps - a volunteer, part-time, cyber security organisation under the jurisdiction of the Australian Cyber Security Centre (ACSC).

Similar organisations exist in the United Kingdom (Joint Cyber Reserve Force), Estonia (Cyber Unit of the Estonian Defence League), and in US States such as Wisconsin and Michigan (Wisconsin Cyber Response Teams and the Michigan Civilian Cyber Corps). An Australian Civilian Cyber Corps, or equivalent, have been suggested by Hon Tim Watts MP, Hon Dan Tehan MP, and Professor Greg Austin (UNSW Canberra Australian Centre for Cyber Security).

The purpose of the Civilian Cyber Corps would be to provide the Australian government with an increased cyber security capability for preparation against cyber attacks, provide training for members, and provide a government-directed incident response surge capacity.
You can find more details on the NISR website.

Securing Democratic Institutions

The increasing social media uptake and decreased information gatekeeping provided through internet saturation, have created the perfect breeding ground for widespread and low-cost information operations.

Research by the Australian Strategic Policy Institute identified 48 public votes (41 elections and seven referendums) between 2010 and 2020 where cyber-enabled foreign interference was reported, and finds that there has been a significant uptick in such activity since 2017.

Democracy is more significant than just government. Many of the institutions we rely on for a healthy democracy fall outside the protection of government networks. Institutions such as political parties, journalists, think tanks, foreign-language media and diaspora groups all play a vital role in the health and resilience of our democracy, and these institutions are under attack. Russian interference in the 2016 US election peaked with the hacking of the Democratic National Committee email system. The 2019 European Union elections were notable because of the widespread targeting of non-government entities such as think tanks and non-profits.

In Australia, the 2021 hack of the NSW division of the Australian Labor Party demonstrates that this is not just a problem for other countries.

The 2019 MYEFO included $2.7m across the 2019-2023 financial years as part of the Cyber Security Resilience and Workforce Package to secure the networks of Australia's largest political parties. The government should consider expanding this funding to include at-risk democratic institutions.

Official Government Position on Takedowns of Cyber Criminal Infrastructure

Ransomware and other financially motivated cyber criminals continue to undertake cyber attacks because they are profitable. The only way to reduce the number of financially motivated cyber attacks is to increase the cost of such attacks or reduce the benefits.

Many serious ransomware operations, including REvil, BlackMatter, and Hive, have either had their infrastructure targeted by state-based offensive cyber attacks or shut their doors with references to expected offensive actions.

While not a silver bullet, these offensive actions add cost to cyber criminal organisations.
The recent 2023 US National Cyber Strategy has indicated a growing willingness of the US government to deploy offensive cyber operations against cyber criminals, indicating that the US government plans to employ "all elements of national power" against cyber criminals.

Similarly, the UK's 2022 National Cyber Strategy includes an objective to "Deter and disrupt state, criminal and other malicious cyber actors and activities against the UK, its interests, and its citizens".

The Australian government has also indicated a willingness to deploy offensive cyber operations against non-state cyber criminals. In 2020, then Minister for Defence Reynolds indicated that ASD had "disrupted activities from foreign criminals by disabling their infrastructure and blocking their access to stolen information". The Secretary for Home Affairs and Director General of ASD have both previously indicated at ASD's offensive operations against cyber criminals. Finally, the current Assistant Minister for Foreign Affairs wrote, in a 2021 discussion paper, that "Australia should seek to impose costs on ransomware crews that target Australian organisations by seeking to disrupt their activities through offensive cyber operations."

Australian and partner governments have demonstrated the capability and willingness to deploy offensive cyber operations against financially motivated non-state actors. In order to maximise the deterrence effect of such operations and to provide Australians with clarity on the government's policy, the government should publicly clarify its position on the use of Australian government offensive cyber capabilities to neutralise the assets/infrastructure of cyber criminals.

End of Appendix