21 April 2023

2023-2030 Australian Cyber Security Strategy Discussion Paper
Submission by email: auscyberstrategy@homeaffairs.gov.au

2023-2030 Australian Cyber Security Strategy Discussion Paper

About us

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

The **UNSW Business School Regulatory Laboratory** ('RegLab') is a community of researchers examining regulation and governance in the UNSW Business School. Reg Lab is a transdisciplinary lab examining the challenges faced by regulators and the regulated in the context of rapidly changing business models. It has a focus on the networked industries sector and data driven innovation. It is jointly funded by the UNSW Business School and external partners (primarily, Google but supplemented by research funding by the Commonwealth).

About this Submission

We are grateful for the opportunity to make a submission on the 2023-2030 Australian Cyber Security Strategy Discussion Paper. Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public.

We respond to questions selectively, focussing on areas where our research might shed light. Our three main points are as follows:

1. **Cyber security and cyber resilience require a shared national strategic vision, supported by laws, policies, advocacy, education, skills, training, and funding.** The government is asking everyone – individuals, families, communities, regions, cities, businesses, not-for-profits, governments – to *opt-in* to that vision. To achieve national alignment and clarity, collaboration, communication, and cooperation will be the crucial mechanisms for success and managing complexity. This requires understanding what is already there (the full complexity of the existing legal and policy framework) before adding new components.

2. **Cyber security, like many other complex fields,[1] exists in *shared regulatory space*.**[2] Overlapping regulatory frameworks, functions and authority are normal in a complex field such as cyber security. Research in Australia and elsewhere demonstrates that the best strategy for mitigating the known harms, and harnessing the known benefits, of regulatory overlap is the use of enhanced coordination and cooperation tools. A new Cyber Security Act could achieve this by engaging directly with the coordination and cooperation challenges of multiple agencies, regulators, departments, and stakeholders. However, in enhancing cooperation and coordination, strong accountability and transparency mechanisms must be hardwired into the regulation.
3. **New mechanisms for reform must aim to improve cyber security outcomes for society, the economy, and the national interest**. A new Cyber Security Act and further amendments to the *Security of Critical Infrastructure Act 2018* (Cth) ('SOCI') provide publicly scrutinised legislative solutions to the problems cyber security policy seeks to solve. While flexibility for government and businesses is important, government must carefully assess the kind of matters that can be decided in delegated legislation (eg, regulations, declarations, notices), or in co-regulatory and self-regulatory mechanisms (eg, codes of practice, guidelines, assessments, standards), and those which belong in the primary legislation due to: their importance to the operation of a legislative scheme; the need for certainty and clarity around obligations; and to support Australia's underlying democratic values.

Questions

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?

We would like to see a focus on co-ordination of law and policy that is built on an understanding of the broad roles that law already plays in this space. Using the example of computer crime laws and vulnerability disclosure schemes, this submission provides a positive example of the benefits of such coordination.

Co-ordination

We would like to see demonstrated, holistic understanding of the role that different parts of the law play in making Australia a cyber secure nation. The policy agenda for cyber security is driven by an ever wider and evolving list of threats and harms, from data breaches to cybercrime to foreign interference to cyber warfare. When cyber security incidents occur in Australia and elsewhere, they enliven multiple legal and regulatory frameworks, and effect civil society, the economy, and the national interest. For example, the Optus Data breach enlivened, inter alia, the *Telecommunications*

[1] Nathan Sales likens regulating cyber security to regulating the environment, competition (antitrust) or public health, recommending that cyber security policy-makers and regulators draw from those sectors for ideas, insights and solutions. See Nathan Alexander Sales, 'Regulating Cyber-Security' (2013) 107(4) *Northwestern University Law Review* 1503, 1507-1509.

[2] Jody Freeman and Jim Rossi, 'Agency Coordination in Shared Regulatory Space' (2012) 125(5) *Harvard Law Review* 1131-1211, 1136.

Act 1997 (Cth) licensing regime,[3] privacy laws, director's duties,[4] financial reporting regulation,[5] and cybercrime.[6] Overlapping and fragmented delegations of power, authority and jurisdiction came into sharp focus during the breach, with multiple regulators acting in response, including the Australian Information Commissioner,[7] the Australian Communications and Media Authority,[8] and the Australian Federal Police.[9] AustLII's Cyber Law Mapping Project and ANU's Tech Policy Atlas illustrates some of the complexity here.[10] One challenge in the government's work on cyber security reform to date is that the reports go into less depth on what is already there (ie the role that law already plays) compared to a typical law reform report. The risk is that what is created will be grafted onto an already complex framework.

While the complexity and connectivity of the existing legal and policy framework presents Australian governments at Federal, State and Territory level with multidimensional overlap problems, it need not be seen as an insurmountable problem. In a cyber security context, law operates offensively, defensively, and structurally, shaping frameworks, authority, delegations, obligations, and behaviour in multiple contexts, from civilian and defence contexts to social, political, and economic contexts. Law operates in sector-specific and cross-sectoral regulatory contexts too, meaning that legal fields, sectors of the economy and regulation overlap, yet also operate independently in distinct jurisdiction and subject matter domains. The existing overlap and fragmentation are not unusual being caused, in part, by Australia's federal structure and, in part, by the nature of cyber security itself.

Improving understanding of the different roles that law plays will assist in creating a sense of *'shared regulatory space'*,[11] which, rather than seeing overlap, fragmentation, and inconsistency in law and policy frameworks as a problem, will encourage, as Freeman and Rossi argue, a focus on the

[3] See, eg, Telecommunications (Carrier Licence Conditions—Security Information) Declaration 2022: <https://www.legislation.gov.au/Details/F2022L00958> and Telecommunications (Carriage Service Provider—Security Information) <https://www.legislation.gov.au/Details/F2022L00959>

[4] See, eg, a cyber security breach may enliven liability for directors under Section 180 of the *Corporations Act 2001* (Cth).

[5] See, eg, AUSTRAC, *Reporting obligations following personal data breaches* (Web Page) <https://www.austrac.gov.au/optus-data-breach-working-our-reporting-entities>.

[6] See, eg, Australian Federal Police, *Operation Guardian expands to combat further cybercrime* (Web Page) <https://www.afp.gov.au/news-media/media-releases/operation-guardian-expands-combat-further-cybercrime>.

[7] Office of the Australian Information Commissioner, OAIC opens investigation into Optus data breach (Press Release, 11 October 2022) <https://www.oaic.gov.au/newsroom/oaic-opens-investigation-into-optus-over-data-breach>.

[8] Australian Communications and Media Authority, 'ACMA investigation into Optus Data Breach' (Press release, 11 October 2022) https://www.acma.gov.au/articles/2022-10/acma-investigation-optus-data-breach.

[9] Australian Federal Police, 'Operation Guardian expands to combat further cybercrime' (Press Release, 28 March 2023) <https://www.afp.gov.au/news-media/media-releases/operation-guardian-expands-combat-further-cybercrime>.

[10] Tools such as Austlii's Cyber Law Map and ANU's Tech Policy Atlas are useful starting points for understanding the shape of the current legal and regulatory landscape.

[11] Freeman and Rossi describe 'shared regulatory space', arguing that while agency coordination is one of the central challenges of modern governance, the nuanced concept of 'shared regulatory space' enables a discussion of coordination tools, practices and techniques that can improve the overall quality of decision making 'by introducing multiple perspectives and specialised knowledge and structuring opportunities for agencies to test their information and ideas': Freeman and Rossi (n 2). 1136, 1210.

interplay between departments' and agencies' delegations, jurisdiction and subject matter expertise; on areas where agencies and departments work at cross-purposes; on ways to capitalise on their unique strengths; and ensure transparency and accountability frameworks are operating appropriately.[12]

To enhance coordination, cooperation, and collaboration in cyber security's 'shared regulatory space', we recommend that the Strategy include:

- Clarity around intragovernmental and intergovernmental coordination and cooperation for cyber security;
- Clarity around delegations of power to administrative agencies and statutory authorities for cyber security;
- Consider *enhanced coordination tools*, such as the creation of a 'Cyber-Reg' for sector-specific and cross-sectoral regulators with jurisdiction, delegation, discretion, or authority over cyber security.

An example: The Cyber Socket proposal[13]

One example where law can point in different directions is the interaction between computer crime laws and vulnerability disclosure programs. This links to a proposal we have worked on with the NSW government, the idea of a 'socket' for vulnerability disclosure schemes within computer crime laws. Currently, computer offences are dealt with federally in the Criminal Code and in equivalent state/territory laws. Ideally, all would be amended as per this proposal since the problem is only resolved if security researchers are protected from prosecution nationally (given that networks cross borders).

Computer offences include offences that are unrelated to broader criminal conduct (eg Criminal Code, Section 478.1). In these cases, the crime could be committed where a person believes they are participating in a vulnerability disclosure program, but their acts are not, in fact, 'authorised' under the terms of that program. This can be the result of poor drafting or innocent misinterpretation.

To give an example of the problem, consider the current intersection of the law and one organisation's program (NAB). NAB's website states 'NAB does not condone malicious or illegal behaviour in the identification and reporting of security vulnerabilities.' It is not clear how this statement intersects with illegality in the Criminal Code – is a person participating in NAB's program required to act within the law (eg not access restricted data held in a computer) as a condition of participation or does participation mean that the conduct is not illegal in the first place (because access is not unauthorised)? Further, what is the consequence when a person is registered for the

[12] Ibid.
[13] See generally The U.N. Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) underlined governments' duty to encourage responsible reporting of vulnerabilities in 2021 (Web Page) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf>; Human Rights Watch letter to the UN Ad Hoc Committee on Cybercrime: 'Too often, security researchers, who help keep everyone safe, are caught up in vague cybercrime laws and face criminal charges for identifying flaws in security systems'(Press Release, 13 January 2022) <https://www.hrw.org/news/2022/01/13/letter-un-ad-hoc-committee-cybercrime>; Riana Pfefferkorn, 'The importance of protecting good faith security research' (Centre for Internet and Society Blog Post, 14 September 2020) <https://cyberlaw.stanford.edu/blog/2020/09/importance-protecting-good-faith-security-research>.

program but misinterprets one of the scope statements? Even where such questions can be answered, people looking to participate in such programs may be nervous about criminal consequences (and lawyers, where they can be afforded and are consulted, may be justifiably cautious given the criminal consequences).

The proposal is to amend the computer crimes legislation to make it clear that those participating in good faith in a vulnerability disclosure program are not guilty of an offence. The laws can be amended to act as a 'socket' into which vulnerability disclosure programs can 'plug in', protecting participants from accidental criminal consequences.

Drafting the changes would be for legislative drafting offices (and different in each jurisdiction), but broadly what could be done is:

- **Define** 'vulnerability disclosure program' – this could be done through a general definition, possibly in conjunction with an 'opt in' where a registry is kept of such programs for the purposes of computer offence laws. One advantage of an 'opt in' system is the creation of a register of programs in Australia, which might be useful to the security community.
  - Ethical hacking is now also being done through AI/algorithms (e.g., CSCRC's Smart Airport project) rather than manually by human individuals. This should be included in the definition of 'vulnerability disclosure program'.
  - Currently, 'ethical hacking' activities are typically governed by standards developed in an ad hoc manner by private agreements (between companies and 'ethical hackers'), as well as by industry norms.[14] These standards ensure respect for business-oriented values (such as the protection of the client companies from harm) rather than societal and ethical values more broadly defined.[15] If a general definition of "vulnerability disclosure program" is made, this could lead to standardising and unifying ethical hacking agreements and industry norms. Given that this proposal promotes the greater social value of encouraging security research, it may be appropriate to emphasise this social value in the definition.
  - If creating an opt-in, conditions could be put on that requiring organisations opting in to agree to meet certain standards on visibility, responsiveness (including transparent timelines), clarity about rewards (recognition or monetary), agreement to make vuln public after a reasonable time etc.
  - One issue to be resolved relates to scope – Is this only for reporting to Australian companies or also to foreign companies (which raises national security issues)?

- **Define** 'good faith participation in a vulnerability disclosure program' (or similar words) if that person has met any registration requirements for the vulnerability disclosure program and they acted:

[14] See, eg, Code of Ethics for Ethical Hackers Certified by US-based organization EC-Council (International Council of Electronic Commerce Consultants) <https://www.eccouncil.org/code-of-ethics/>

[15] Jaquet-Chiffele, David-Olivier, and Michele Loi, 'Ethical and Unethical Hacking' in Markus Christen, Bert Gordijn, and Michele Loi Cham (eds.) *The Ethics of Cybersecurity*, (2020, Springer) 179–204.

  - in good faith for the purposes of testing, investigating and promptly reporting a security flaw or vulnerability, in the reasonable belief that their actions were within the terms of a vulnerability disclosure program;
  - without intending to or threatening to cause harm to persons, property or systems.

- **Choose** mechanism that protects those participating in good faith in a vulnerability disclosure program from prosecution:
  - Option 1: Specify in definitions that conduct that is good faith participation in a vulnerability disclosure program is taken to be authorised.
  - Option 2: Create a defence to relevant offences where the conduct that would otherwise constitute the offence is within the definition of "good faith participation in a vulnerability disclosure program".

There are other legislative frameworks that provide a level of protection/immunity for those engaging in authorised activities, including testing systems and equipment and technical assistance for authorised activities. These include:

- *Telecommunications (Interception and Access) Act 1979* (Cth) s 6AAA
- *Telecommunications Act 1997 (Cth)* s 279; Pt 15 Dvs 2, 8
- *Surveillance Devices Act 2004* (Cth) (SDA) s 65A.

The example not only provides a useful law reform but illustrates the benefits of coordination across different legal domains. Incentivising vulnerability disclosure schemes also needs to consider perceived legal obstacles such as computer crime laws.

2. What legislative or regulatory reforms should Government pursue to enhance cyber resilience across the digital economy?

a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

Legislation provides a crucial publicly scrutinised structural frame, which is appropriate for identifying regulatory scope (for example, SOCI identifies what constitutes critical infrastructure and outlines the powers and responsibilities of the Minister, relevant agencies, regulators, and departments) but not necessarily for providing detailed technical guidance or the required flexibility to respond to a cyber incident. However, despite the known limitations of legislation, the government must carefully consider the kind of matters that can be decided in delegated legislation or other mechanisms (such as co-regulatory or self-regulatory mechanisms), and those which belong in the primary legislation due to their importance to the operation of a legislative scheme.[16]

Beyond specific legislation mentioning 'cyber security' explicitly, both general legislation and the common law can have a positive impact on cyber security. For example, tort law and consumer law

[16] See, eg, comments of the Standing Committee for the Scrutiny of Bills concerning the Security Legislation Amendment (Critical Infrastructure) Bill 2020, *Scrutiny Digest 5 of 2021*, 103.

provide incentives and set out general requirements that impact on cyber practices. To give an example, a company selling internet-connected self-driving cars would be exposed to significant legal risk should those cars be able to be hacked and controlled by a third party. This is not because we have legislation on "cyber security for vehicles", but rather because of general tort liability and consumer law protections (eg hackable vehicles would be unsafe and unfit for purpose).

Regulatory guidance can be a useful mechanism for aligning with international cyber security standards. For example, legislation might set a requirement for risk management or a requirement to store data securely, but regulatory guidance might then indicate that compliance with one of a range of accepted international standards (for risk management or data storage respectively) would meet that general requirement.[17] This provides organisations with flexibility, particularly where they operate in more than one jurisdiction, over more specific legislated Australia-specific requirements. At the same time, government can encourage organisations to follow particular standards as a known means of meeting the legislated standard.[18]

There is a need to break down the silos between system protection and data protection. In practice, cyber security is the protection of both systems and data concurrently. This is particularly true in the case of critical infrastructure. The Optus, Medibank and Latitude Financial incidents involved data breaches, but may have a comparable impact on confidence in critical infrastructure as system breaches. In this sense, the *Privacy Act 1988* (Cth) is part of the web of laws that regulate for cyber security.

b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

The extension of SOCI to 'data' and 'systems' will require extensive consultation as 'consumer data' and 'systems' are open, evolving categories. Data as a term is rarely defined in legislation and there is a risk that definitions will trap concepts in current understandings. For example, data is often described as 'digital' even though quantum computing may change the format in which data is stored and analysed. Any legislative definition must aim – as best as it can – for language aligns with legislative goals as technology evolves (which might be described as 'technological neutrality'). Yet, at the same time, legislation must also fully integrate protection of consumer privacy and mitigate against 'purpose' and 'use' creep by agencies and regulators. The definitions of 'data' and 'systems' in this context will be paramount.

There is current regulatory activity examining issues associated with quality of data which may be helpful in these definitions.[19] The roles of both Treasury and the Australian Competition and Consumer Commission in the Consumer Data Right include addressing such concerns.

[17] The *Security of Critical Infrastructure Act 2018* (Cth) ('SOCI') already accommodates this, however, there is scope to improve the 'equivalence' provisions.

[18] See eg, Section 30AN(3), SOCI.

[19] ACCC, 'Data Quality in the Consumer Data Right' (Web Page) <https://www.accc.gov.au/system/files/Data-Quality-in-the-Consumer-Data-Right-Findings-from-Stakeholder-Consultation.pdf>.

c. Should the obligations of company directors specifically address cyber security risks and consequences?

Company directors already have general obligations that implicitly include identifying and managing (cyber) risk.[20] Additionally, sector-specific legal requirements may require directors to identify and manage cyber security risks and consequences in particular ways. For example, the Australian Securities and Investments Commission action against RI Investments[21] demonstrated that directors and officers of corporations that hold an Australian Financial Services Licence, may be at risk of personal liability if the licensee contravenes the *Corporations Act 2001* (Cth) because of having inadequate cybersecurity or cyber resilience. General "specific" requirements may not be necessary, although guidance may be useful but, if introduced, should avoid doubling up with what already exists.

D. Should Australia consider a Cyber Security Act, and what should this include?

A *Cyber Security Act* that focuses on delegations, and intra- and inter-governmental cooperation and coordination may alleviate some of the issues present in the current governance, legislative and regulatory frameworks. Regulatory overlap literature suggests that governance, legislative, regulatory, jurisdictional, and subject matter silos contribute to problems of coordination and cooperation.[22] A common theme identified in the literature is the need for coordination and cooperation tools, regardless of whether the regulatory overlap is considered desirable or undesirable.[23] In the EU, the *Cyber Security Act* fulfils this role; the EU Agency for Cybersecurity undertakes operational cooperation at EU level and supports coordination of large-scale cross-border cyberattacks and crises.[24] Additional legislation proposed in the EU seeks to strengthen coordination and cooperation for, among other things, cyber security crisis management, threat detection and response capability.[25]

e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

A starting point would be to determine the extent of legal, regulatory, and jurisdictional overlap between departments, agencies, and sector-specific and cross-sectoral regulators. Research suggests that in some circumstances, regulatory overlap is desirable as it creates redundancy.[26] Importantly, agencies, regulators and departments can still operate effectively and efficiently if their

[20] Cyber security incidents and data breaches may attract liability under Section 180 of the *Corporations Act*.
[21] *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* [2022] FCA 496.
[22] Lachlan Robb, Trent Candy and Felicity Deane, 'Regulatory Overlap: A Systematic Quantitative Literature Review' (2022) *Regulation & Governance* <https://doi.org/10.1111/rego.12504> .2
[23] Lachlan Robb, Trent Candy and Felicity Deane, 'Regulatory Overlap: A Systematic Quantitative Literature Review' (2022) *Regulation & Governance* <https://doi.org/10.1111/rego.12504> . 16
[24] See European Commission, 'The EU Cybersecurity Act' (Web Page) <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>.
25 See European Commission, 'Cyber: towards stronger EU capabilities for effective operational cooperation, solidarity and resilience' (Press Release, 18 April 2023) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2243
[26] Todd S Aagaard, 'Regulatory Overlap, Overlapping Legal Fields, and Statutory Discontinuities' (2011) 29(3) *Virginia Environmental Law Journal* 237-303,. 241

functions do not overlap, even if their jurisdiction, delegations, or authority overlaps. For example, centralising certain functions, such as information-gathering, can operate effectively with other decentralised functions, such as program implementation.[27] This largely exists in the Australian case already, with different agencies, departments and regulators having different authority, jurisdiction, and functions regarding policy, laws, and regulation that contribute to cyber security.

Ways to streamline existing regulatory frameworks[28] may include better coordination between agencies in areas of overlapping authority, delegation, and jurisdiction. It may be fruitful to examine the structures, jurisdictions and relationships among agencies, regulators, and departments to get a better picture of their role in 'shared regulatory space'. That said, some agencies must maintain independence – law enforcement and security agencies in particular – because their functions require additional scrutiny and oversight.

There are opportunities to streamline existing regulatory frameworks. For example, the SOCI Act already provides a flexible model for using risk management standards in the context of critical infrastructure protection.[29] This model could go further by providing a greater range of national and international standards that can be used by industry participants to meet their cyber security obligations. This could be achieved by permitting the use of standards to meet the required legal requirements, including international and internationally recognised best practice standards.

f. 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?

This is a difficult question and one on which opinions vary, in part because the impacts of such a prohibition are unknown. Might it cost lives? Would it reduce cybercrime? Would it disincentivise breach notification and information sharing? One option would be to test a prohibition in a particular sector to observe its impact before making changes nation-wide.

There is an essential policy balance between eliminating the business model behind ransom cybercrime and ensuring that breach notification is not discouraged. In practice, the insurance sector can provide rich analysis of their experience of this balance. Analysing insurance data may indicate whether paying a ransom provides access to data and whether that data is retained and monetised by the cybercriminal regardless of payment.

[27] Alejandro E Camacho and Robert L Glicksman, 'Designing Regulation Across Organizations: Assessing the Functions and Dimensions of Governance' (2021) *Regulation & Governance* <https://onlinelibrary.wiley.com/doi/10.1111/rego.12420>. 24

[28] We define regulatory frameworks inclusively, comprising laws and legislation, regulation, co-regulatory, self-regulatory, and voluntary mechanisms. For example, in complex sectors of the economy, such as critical infrastructure, it is commonplace to have multiple regulatory mechanisms in operation from voluntary to mandatory.

[29]Part 2A, Section 30ANA of SOCI

i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

This is currently unknown. The goal would be to reduce cybercrime, but it might also reduce reporting and information sharing or lead to death (for example, in the context of a hospital highlighted by the WannaCry ransomware attack on the UK National Health System). Much depends on how the cybercrime sector would respond, if at all, to a prohibition, and that is largely unknowable without testing (and, even there, they might respond differently to a test than to a nation-wide prohibition being implemented and enforced).

g. Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

Yes, the Australian government should clarify its position with respect to payment or non-payment of ransoms. Currently, there are legal risks in paying ransoms, in particular where (1) a person is reckless or negligent as to whether the money will be used as an instrument of crime, (2) funds are intentionally made available to a terrorist organisation where the person is reckless as to whether the organisation is a terrorist organisation, or (3) where the transfer of the ransom is affected by a UN Security Council sanction. Given that ransoms are often paid to organisations that use the funds for crime or terrorism or are based on sanctioned jurisdictions, it is difficult terrain to navigate. Legal clarity will help organisations make decisions that do not fall foul of the law but are otherwise in the best interests of the organisation.

However, it is important that the clarification does not lead to further regulatory burden. For example, clarification that paying some forms of ransom might be in breach of Anti-Money Laundering and Counter-Terrorism Funding (AML/CF) will attract the jurisdiction of AUSTRAC, with significant impact on AUSTRAC's reporting entities.

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

Standards Australia, in partnership with other national standards bodies through the International Standards Organisations and similar bodies, develops international standards on a range of matters, including in relation to cyber security. Participation in Standards Australia committees is often easier for industry than for other sectors such as government, NGOs and academia. In particular, participation is effectively voluntary and can cost money, including for travel to international meetings. In cyber security and other matters, government could provide more support to broaden participation in standards development and enhance Australia's voice internationally.

There are different standards-making bodies, and the conflict with intellectual property may vary among them. In some circumstances, it may be preferable to rely on bodies such as the OECD where the role of industry is reduced. The OECD has recently produced a report on privacy enhancing technologies that is a precursor to standardisation.

Responsible state behaviour is a different question, and outside the scope of this submission.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

The Commonwealth Government does not have as strong a track record on areas where cyber security is a significant issue. The Australian National Audit Office has undertaken a number of cyber security related performance audits in the last 5 years which document areas for improvement for government, including reviewing cyber resilience of the Department of the Treasury, National Archives of Australia and Geoscience Australia,[30] the cyber security strategies of non-corporate government entities, including Department of Home Affairs and the Australian Signals Directorate,[31] and the management of cyber security supply chain risks by Department of Foreign Affairs and Trade and the Australian Federal Police.[32] In regard to data management, the evidence given in the Robodebt Royal Commission indicates that there are significant problems in data management as well as data systems management. Sadly, best practice is rarely found in service delivery Commonwealth Government departments.

Commonwealth Government departments could have a great deal to offer in the co-design of cyber security best practice models. For example, the Commonwealth Government has significant experience in managing applications programming interfaces (APIs) through its work on the Consumer Data Right. In these areas, the Commonwealth Government can act as an exemplar of best practice and can use its experience to provide guidance to both other levels of government and to industry.

However, most Commonwealth Government departments are not operating at the best practice level. It is essential that this changes. To prematurely claim to be at best practice is likely to lead to much poorer cyber security outcomes than acknowledging that all entities, including most Commonwealth Government departments, are on a common path to improving cyber security. The ANAO's proposal to audit cyber security management across several entities, as a continuation of its cyber security audit program, is a welcome and necessary initiative.[33]

7. What can government do to improve information sharing with industry on cyber threats?

Greater real-time or near real-time information sharing for cyber security offers benefits to both industry and government. The Trusted Information Sharing Network (TSIN) is a stable, functioning model (and platform) for government and critical infrastructure business information sharing. Other information sharing and business liaison models exist within agencies and regulators that are effective for sharing information in sector-specific or issue-specific contexts.[34] However, given that

[30] See Australian National Audit Office, Cyber Resilience, Auditor-General Report No. 53 of 2017–18 <https://www.anao.gov.au/work/performance-audit/cyber-resilience-2017-18>.

[31] See: Australian National Audit Office, *Cyber Security Strategies of Non-Corporate Commonwealth Entities*, (Auditor-General Report No. 32 of 2020–21) <https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities>.

[32] See Australian National Audit Office, *Management of Cyber Security Supply Chain Risks* (Auditor-General Report No. 9 of 2022–23) <https://www.anao.gov.au/work/performance-audit/management-cyber-security-supply-chain-risks>.

[33] See Australian National Audit Office, *Management of Cyber Security* (Potential audit: 2022-23) <https://www.anao.gov.au/work/performance-audit/management-cybersecurity-0>.

[34] The Australian Security Intelligence Organisation's outreach functions are an example of sector-specific and cross-sectoral information sharing. See ASIO (Web Page) <https://www.asio.gov.au/outreach>.

cyber security incidents and episodes cut across business, community and national interests, there is an obvious tension between disclosure of industry and government's confidential and secret information on the one hand, and managing its use and dissemination on the other. Businesses and government are both concerned about this aspect of information sharing.

As a starting point, we recommend reviewing the horizontal (inter-governmental and sector-specific) and vertical (intra-governmental and cross-sectoral) information sharing mechanisms across regulatory frameworks and within government. A review would provide insight into where overlapping and fragmented information sharing exists, where there is desirable redundancy, what the shared regulatory spaces are, and which legal, operational, communication and coordination tools would assist government and industry in strengthening cyber security practices and improving information sharing. Some delegations and redundancies are constitutional in nature, and some are jurisdictional, delineated by discrete legal and regulatory fields (consumer law, company law, energy regulation, telecommunications, security of critical infrastructure, etc).

One solution is to apply the concept of co-design more assertively than it was in the SOCI reform discussions. By this we mean using co-design to review and improve existing information sharing processes and potentially to design new processes. During the SOCI reform process, co-design was used to formulate the critical infrastructure risk management program (CIRMP) rules created under the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*. The purpose of the co-design process was to engage levels of government and sector-specific critical infrastructure industries in the risk management program rule design. The stated goal was to leverage existing frameworks, regulation, and guidelines, and reduce duplication, cost, and the regulatory burden of compliance.[35] Co-design therefore has the prospect of reducing inconsistent obligations between regulatory frameworks. Several reviews are underway at the moment that will impact information sharing, such as the review of secrecy laws[36] and privacy laws[37]. The recommendations of these reviews would need to be considered in any co-design process for developing more efficient information sharing. We have also published an article that explains some information sharing challenges (not specifically related to cyber security) in terms of unnecessary legislative complexity.[38]

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?

Creating a mutual obligation of confidentiality about information shared during a cyber incident is not a major issue *contractually*. It would be straightforward to put an arrangement by deed or

[35] Explanatory Memorandum, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 287.

[36] See Attorney-General's Department (Web Page) <https://www.ag.gov.au/crime/publications/review-secrecy-provisions>.

[37] See Attorney-General's Department (Web Page) <https://consultations.ag.gov.au/integrity/privacy-act-review-report/>.

[38] Lyria Bennett Moses 'Who Owns Information? Law Enforcement Information Sharing as a Case Study in Conceptual Confusion', (2020) 43 *University of New South Wales Law Journal* 615 - 641 <https://search.informit.org/doi/10.3316/agispt.20200710033134>.

agreement in place. In effect, a change to providing explicit confidentiality obligations is merely to change the *status quo* from an obligation on the organisation with the potential for a breach to ASD and ACSC to a mutual confidentiality obligation.

However, a confidentiality regime requires further deliberation as it raises legal and ethical issues around entity reporting, disclosure, and other sector-specific and cross-sectoral statutory obligations. For example, if ASD or ACSC receive confidential information which individuals are obliged to report to the relevant regulator, how that can confidentiality be maintained? While there are mechanisms in the *Telecommunications Act 1997* (Cth) and *Telecommunications (Interception and Access) Act 1979* (Cth) which provide limited immunity to carriers and their staff members to assist law enforcement agencies,[39] in the broader context of information sharing, secrecy and confidentiality can impede cooperation and communication. A confidentiality arrangement between ASD and ACSC and an organisation may have unintended effects on the operation of other regimes, or operate contrary to reporting regimes or acceptable standards, which apply to the organisation, especially if that entity is a critical infrastructure entity.

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?

There is some possibility that notification would assist the public. However, it is much more important that the notification assist other stakeholders of the entity that has been the subject of the incident. For example, shareholders of a public company should reasonably expect that mandatory reporting of ransomware is part of continuous disclosure. Vendors and customer of a corporation should understand the risks associated with the cyber security of their customers and suppliers respectively. Communication plans and strategies can also be employed to manage communication to the public in a timely and sensitive manner. Crisis management literature and practice could be drawn upon to develop guidelines on notification and communications around these issues.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Cyber security is not exclusively a 'technical' problem. There are technical elements (for example, the mathematics underlying the security of encryption and hashing protocols), but increasing STEM skills in general will not, of itself, generate a cyber security workforce.

Improving cyber governance and practices within organisations will require people working in a range of roles to have a range of skills. For example, those seeking careers as managers or entrepreneurs will need skills in understanding governance obligations and cyber risk for their context and building a strategy to meet legal requirements and manage risk. That strategy might include employees or external service providers, but they will still need to ask the right questions.[40]

[39] A new approach could mirror or adapt these provisions. See Part 15 of the *Telecommunications Act 1997* (Cth), and Chapter 2 of the *Telecommunications Interception and Access Act 1979* (Cth)
[40] See, eg, Australian Cyber Security Centre, Questions for Boards to Ask about Cyber Security (Web Page) <https://www.cyber.gov.au/acsc/view-all-content/publications/questions-boards-ask-about-cyber-security>.

More broadly, even in primarily HASS fields, people will need skills related to cyber governance, including specialist skills where relevant in, for example, relevant legal frameworks, security risk management, and human psychology. Other fields, such as history and philosophy, can also enhance understanding of cyber-related challenges.

There are other skills that are crucial in a cyber context and are relevant across all fields, including those gaining specific technical secure programming and networking skills. One example is the ability to engage in “security thinking”, adopting an “attacker mindset” to identify vulnerabilities in a particular socio-technical system (like an organisation’s computer systems and the humans using them). These skills do not fit neatly into a STEM/HASS divide and, in the real world, often require people with different skills working together.

At UNSW, we not only have Engineering courses, such as those offered through SecEDU, we also incorporate cross-disciplinary courses and include, where relevant, non-STEM courses or modules in programs for future cyber security professionals. For example, students in an online cybersecurity masters program study cyber ethics and can choose to study cyber law.

In short, STEM skills are critical across the economy, but that agenda alone is insufficient for uplifting cyber skills for all the roles where they will be required.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

A single reporting portal is a reasonable aspiration. This could allow for information collected to be passed on to relevant regulators on the back-end, with some questions asked conditionally (eg questions relevant to critical infrastructure are only asked where relevant).

However, it is important to continue with existing and evolving reporting obligations while the portal is established. One way of dealing with this, pending creation of a single reporting portal, would be to have a “no wrong door” approach between regulators and an obligation on each regulator to provide information to a central and reporting body and/or each other. This body may be one of the regulators. The “no wrong door” approach is already being operated by the regulator members of the Digital Platforms Working Group (DG-WP). As a stop-gap measure, government should avoid criticising entities for reporting in the ‘wrong’ place or not all of the ‘right’ places.

14. What would an effective post-incident review and consequence management model with industry involve?

An effective post-incident review would, at a minimum, include the following steps:

- Consider carefully the information being reported. Identify the areas of overlap, duplication, fragmentation and redundancy. This provides insight into the nature of incidents being reported, and who has jurisdiction or delegation to deal with them.
- Areas of duplicated regulation (reporting) may only require better coordination, classification, and dissemination. A single reporting portal simplifies reporting. It would be

important to ensure that the backend classification and analysis was accurate, and able to classify incident characteristics with accuracy and specificity.

- To the extent possible, post-incident reviews should be in a form that is useful to others that might be affected. This may be by publication or might be by the confidential sharing of review outcomes.

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

a. 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 need government to provide information to help them identify and manage cyber security risks. We produced a brochure, through the Cyber Security Cooperative Research Centre in partnership with the Department of Home Affairs, aiming to provide such information to SMEs in the supply chain for critical infrastructure. Such advice could also be extended, with some adaptation, to SMEs more broadly.

One of the critical issues is to ensure that SMEs are not left with responsibility for cyber security that they cannot manage. This is an area where state and Commonwealth governments can be proactive. Sheeting cyber security responsibility by contract to SMEs does not reflect supply chain cyber security best practice. There is a need for government contracts to reflect risk, including reputational risk, in contracts with SMEs.

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?

Supply chain cyber security best practice could be employed as part of the Commonwealth procurement process. However, it would require a recognition that cyber security risk is shared, despite contractual agreements that state otherwise. The recent breach at Latitude Financial provides an example. The breach occurred at two service providers. Latitude Financial almost certainly sheeted cyber risk to each of these service providers as part of their supply contracts. However, the reputational damage done was to Latitude Financial itself and not the service providers.

The Commonwealth can lead all levels of government in recognising supply chain cyber security risk in its approaches. This will benefit all vendors, but particularly Australian cyber security firms that can provide localised advice to both domestic and international vendors. The challenge will be for the Commonwealth to recognise that any cyber security breach in its supply chains will create reputational risk at the Commonwealth level. By working with vendors at all points in the supply chain, the Commonwealth can improve national supply chain cyber security. It will need to include best practice on at least:

- risk assessment;
- security policies;
- access control;

- secure communication;
- incident response planning;
- continuous monitoring;
- audits; and
- employee training.

The capacity building that will be required in Commonwealth procurement is high. The result of that capacity will be a significant improvement in Australian supply chain cyber security.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

The best way to manage any policy goal in the context of an evolving socio-technical landscape is careful drafting. In particular, language should align as closely as possible to purpose and avoid non-productive technological specificity. In other words, technological specificity is appropriate only where a particular technology or practice is itself closely aligned with purpose (as in the case of a prohibition on human reproductive cloning or particular kinds of weapons). Reference to 'cyber security' where 'security' is the goal; reference to 'digital' where the format is irrelevant can all be examples of unnecessary technological specificity. For further examination of these issues, see Lyria Bennett Moses 'Regulating in the Face of Socio-Technical Change', in Brownsword R; Yeung K; Scotford E (ed.), *Oxford Handbook of the Law and Regulation of Technology*, Oxford University Press, 2017.

In addition, it is important to recognise the significant advantage of generally worded legislation and common law in the context of technological change.[41] Tort law, consumer law and similar legal frameworks rarely become obsolete in the context of technological change and can play an important role in cyber security; they provide incentives that operate across technological contexts. Their role needs to be recognised as part of a comprehensive map of how law regulates for cyber security.

Liability can be an effective means of creating incentives for better cyber practices. A strict liability regime – where companies paid $100 (say) to each person impacted by a data breach – would incentivise timely data deletion and better cyber security practices across the board. It would give companies flexibility on technological means but would transfer the risk of data breach from individuals to those best able to mitigate it. Factoring in the possibility of cyber insurance, this could create more immediate consequences for good practices, with pricing likely to be depending on the volume of data stored and security practices deployed. Such a regime would, like tort and consumer law, operate in a technology neutral way.

20. How should government measure its impact in uplifting national cyber resilience?

In Australia, there already exists a rich and diverse community of organisations and professionals developing novel, innovative and reliable ways of measuring different kinds of impact, including

[41] Lyria Bennett Moses, 'Adapting the Law to Technological Change: A Comparison of Common Law and Legislation', (2003) 26 *University of New South Wales Law Journal* 394 – 417.

social impacts and outcomes.[42] The government should consider engaging with this community of experts and practitioners to develop fresh, workable, inclusive impact measurement methods, tools, and practices, through partnerships, research, and collaboration. For example, in the area of combatting cybercrime, the United Kingdom has the National Cyber Resilience Centre.[43] The government may also consider creating a national cyber resilience centre for impact or harnessing the skills, expertise, and methodologies of existing experts.

Many organisations, including government and industry, make the (reasonable) mistake of measuring outputs, rather than outcomes. Outputs still matter, but outcomes are what demonstrate social, cultural, organisational, or behavioural change. Uplifting national cyber resilience will require a mix of cultural, behavioural, and material changes to the way individuals, organisations, communities, business, and governments approach the 'cyber' in what they do daily and habitually. Ways of measuring impact will need to include relevant metrics,[44] and focus on the ways to achieve cyber resilience, not only focussing on the consequences of a cyber-attack or system failure.

For example, the Centre for Social Impact's *Australian Digital Inclusion Index*, [45] which tracks the *digital divide* in Australia, provides a potential model for tracking issues and trends that are relevant to cyber resilience and security. Hypothetically, an Australian *Cyber Resilience Index* may seek, among other things, to correlate low levels of digital ability with low levels of cyber security awareness, and low cyber resilience. Conversely, high levels of digital ability may correlate with high-risk cyber activities, or increased awareness and high resilience. This information could be useful for policymakers to inform government about initiatives for education, training, and skills.

Measuring cyber resilience in organisations is also important. The World Economic Forum has recently published white paper for a cyber resilience index for organisations.[46] This is an example of a framework for measuring cyber resilience within organisations and describes relevant metrics to use.

[42] See, eg, the Centre for Social Impact (Web Page) <https://www.csi.edu.au/>.
[43] See National Cyber Resilience Centre (Web Page) <https://nationalcrcgroup.co.uk/>.
[44] ENISA recommends starting with a small number of well-defined, achievable metrics to measure resilience. See European Network and Information Security Agency, *Measurement Frameworks and Metrics for Resilient Networks and Services: Challenges and Recommendations*, ENISA 2010, 11. See also recently on use of outcomes-oriented metrics in a cyber resilience and security context: European Union Agency for Cyber Security, *Building effective governance frameworks for the implementation of national cybersecurity strategies*, ENISA February 2023. See also World Economic Forum, *The Cyber Resilience Index: Advancing Organizational Cyber Resilience - White Paper*, WEF July 2022 <https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf>.
[45] Centre for Social Impact, *Measuring Australia's Digital Divide- Australian Digital Inclusion Index 2016* (Web Page) <https://assets.csi.edu.au/assets/research/Australian-Digital-Inclusion-Index-2016-Report.pdf>.
[46] World Economic Forum, *The Cyber Resilience Index: Advancing Organizational Cyber Resilience - White Paper* (WEF, July 2022) <https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf>.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

The relevant evaluation measures must be something other than tracking the number of incidents. Even tracking the number of people affected by each incident does not provide sufficient public transparency to be of great value. That is, a simple metric-based dashboard is not enough.

Instead, we recommend that the Commonwealth should publish regular public progress reports outlining what has been achieved so far and what still needs to be done. These reports should provide detailed information about the current state of cybersecurity measures, including descriptions of incidents or breaches that have occurred. This would also complement the existing public reporting options.

We also favour independent reviews. This could be an ongoing role for the successor to the Expert Group and would conduct regular reviews of the cyber security measures in place. It must report findings publicly. It would also need to publicly set out areas where improvements can be made. The result would be public confidence in the effectiveness of the cyber security measures.

Yours sincerely,

Lyria Bennett Moses

Susanne Lloyd-Jones

Rob Nicholls