1 March 2024

Department of Home Affairs
Australian Government
By webform: https://www.homeaffairs.gov.au/help-and-support/departmental-forms/online-forms/cyber-security-legislative-reforms-form

Consultation Paper
2023-2030 Australian Cyber Security Strategy: Legislative Reforms

About us

The **UNSW Institute for Cyber Security** ('IFCYBER') has the mission to apply multi-disciplinary and cross-faculty research and teaching partnerships to address sovereign interests and Cyber Security socio-technical problems. IFCYBER is a large conglomerate of 140 experts in cyber security across each of our faculties. Unique to UNSW is our understanding that cyber security is multidisciplinary. We are interested in the human, organisational, social, economic, legal, and technical aspects of cyber security. Our aim is to consider 'real-world problems' and deliver 'real-world impact' – in Australia and globally.

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/.

About this Submission

We are grateful for the opportunity to make this submission. Our submission reflects our views as researchers; they are not an institutional position. We focus on areas related to our research. This submission can be made public.

Measure 1

Responsibility. In terms of responsible entities, we agree with the recommendation that responsibility for compliance should lie with all the vendors, suppliers, importers and manufacturers in the supply chain. However, we note that those further down the supply chain (such as distributors) will need to rely on representations of those further up the supply chain. The legislation should be clear as to the relevance of reasonable reliance and the potentially more limited responsibilities of those who so rely. For example, it could be made clear in the mandatory Code that consumers need only return non-compliant goods to the retailer to receive a remedy, and there

should be no obligation on consumers to deal with others in the supply chain (unless, for example, the retailer has become insolvent).

Scope/Definition. As there are many different and unreconciled definitions of smart devices and similar technologies, a broad definition with (justifiable) exceptions made by subordinate legislation would provide the best protection for consumers. We agree that the definitions of 'connectable products' currently used in ss4-6 of the *Product Security and Telecommunications Infrastructure Act 2022* (UK) appear to meet these requirements. However, we would also urge that those excepted under the legislative scheme nevertheless be required to meet a more general baseline 'reasonable security expectation', so there is no gap in protection. Note that the current *Privacy Act 1988* (Cth) cyber security obligations in the Australian Privacy Principles only apply to personal information, and cyber security breaches can be harmful, particularly in the case of smart devices, without involving personal information.

Whether a particular smart device should be covered by the mandatory cyber security standard depends on various factors including the purpose of the smart device, connectivity, and data it collects, stores, and processes, potential security risks, and impact on human safety from a cyberattack. For example, basic kitchen appliances such as toasters and blenders that have minimal or no connectivity to the Internet might be excluded from a mandatory cyber security standard.

ETSI EN 303 645 The first three principles covered for cybersecurity for the consumer side of IoT devices in the standard ETSI EN 303 645 are a reasonable starting point as the majority of cyberattacks aim to target weak passwords and unpatched security updates. However, there are additional considerations.

If Australia wishes to be a 'world leader' in cyber security, compliance with just the first three security principles in ETSI would be inadequate. In particular:

- Alignment with the strictest standards in a substantial international market would provide better protection. For example, the 2022 draft of the Essential Cybersecurity Requirements in Annex I of the EU Cyber Resilience Act (CRA) went well beyond those three principles. We note that the CRA final form is yet to be released, but examination of the in-force version of those requirements should be encouraged before a final decision is made.
- Coordinated vulnerability disclosure policy for device manufacturers, software developers and support personnel, and component suppliers would make these entities also responsible to comply with patching updates as part of IoT device security management.
- Data protection provisions for consumer IoT should also be considered as a baseline requirement considering the existence of laws such as Europe's GDPR that regulate the protection of personal information of users of IoT devices.
- In addition to cyber security and personal privacy, human safety forms a key criterion towards designing mandatory security standard for IoT and smart devices. Attacks on IoT devices with poor security can impact the delivery of essential health care, home security and other services. For example, attacks on vulnerable smoke detectors and door locks can compromise safety of the people.
- Quantum resilience poses a huge challenge that requires plans to transition to quantum-safe systems.

However, we acknowledge that it is unlikely that products will be manufactured specifically for the Australian market, and that may affect the practicability of imposing stricter standards on products imported into Australia. Thus, noting the need to remain in step with the international market, we agree that Australian standards should align with international standards or that compliance with international standards be otherwise considered sufficient.

If ETSI is used in one form or another, the form in which it is implemented into the Code should be considered carefully. The UK has transposed the current obligations in the standard to their statutory instrument. However, this means that they do not benefit from the potential flexibility of the standard, which could be updated as new threats and solutions are identified. If the government funds a continuing strong Australian presence (including supporting participation by consumer rights organisations) in the development of international standards, it may make more sense to rely on such standards directly. Additionally, to support industry flexibility, referring to one standard is insufficient: we propose that reference to standards in the Code should include 'equivalent' standards.

Regulatory Powers Act. We have no objection to the use of the *Regulatory Powers Act (Standards Provisions) Act 2014* as a regulatory model. However, we suggest appointing an independent professional regulator, like the ACCC, to administer this aspect of the proposed reforms.

Measure 2

Reporting obligations have an important role to play in incident response, accountability, and threat intelligence as well as broader sharing/learning across all sectors. However, as noted in the paper, the combination of reporting requirements adds unnecessary complexity to the challenging task of incident response. In particular, there are separate portals for reporting including SoCI/ACSC, ACSC (general), OAIC, AFP, ScamWatch, eSafety, as well as state-based reporting mechanisms. While these deal with different kinds of scenarios, the overlap and multiplicity are unnecessary. It would be preferable to have a unified portal for reporting incidents, with agencies notified of matters relevant to them depending on the pathway taken in the reporting process. This single reporting platform could then easily extend to ransomware reporting with less regulatory burden than imposing a separate requirement.

Liability/accountability. We agree with the proposal that entities must continue to meet existing legal obligations so that reporting does not preclude liability or accountability. Security has a cost and organisations will only incur such costs if there are also financial risks associated with poor security. Liability is one way to ensure that the risk of a security incident does not lie solely on end users but is also borne by the organisation in the best position to avoid the harm.

Threshold criteria for reporting obligations need to be considered carefully given that SMEs contribute significantly to the economy and have become an attractive target for ransomware. If there is a threshold for mandatory participation, incentives might be offered for voluntary participation by SMEs.

Details. Obligations should also indicate what kind of information should be reported, such as: date, time of attack, amount of ransom, source of the message, mode of payment, due date, and the estimate of loss if the ransom is not paid.

Measure 3

Limited use obligation v safe harbour. This measure seems sensible and is a preferable approach to 'safe harbour' given the obligation to meet legal obligations remains. However, confidence in the arrangements will be critical and will hinge on transparency around how information is used. Organisations may also seek verification where regulatory action is taken that reported information was not used. Documentation regarding the source of information used to initiate and during investigations should thus be retained. However, verifying to the affected party that information was *not* used is technically difficult. A rigorous, trusted oversight mechanism (with full access to internal files) can build confidence in the overall arrangements.

Learning from shared information. Government and regulatory agencies should ensure that the information gleaned is used effectively. They should analyse cybersecurity incidents including ways in which further legal or regulatory changes would better protect against such incidents in the future as well as ways in which alternative mitigation strategies would prevent such an incident from reoccurring.

Measure 4

Need for detail. We agree with Measure 4, although some of the details will be critical including: (1) broad representation in terms of expertise, experience and sector, (2) a process to manage conflicts given competitor, customer, supplier relationships with affected entities, (3) relevance of deliberations and findings for regulatory action (in other words, the meaning of 'no fault'), and (4) the process through which findings are used to prevent and/or mitigate future incidents.

Measure 5

Duplication. One of the issues being considered in the privacy law review is whether more prescriptive rules are required around data storage. There are already specific rules that apply to some entities through other laws as well including those in the consumer data right ecosystem, those entering government contracts (federal or state) as well as foreign legal obligations and including the pressure to comply with international standards. None of that prevents Measure 5, but it does highlight the need to ensure that the obligations are framed so as not to create duplicative obligations or impose similar requirements in slightly different ways thus unnecessarily increasing organisations' compliance burden. This is not only a question for these reforms, but also to reflect on what is done here back on what might be done elsewhere (such as in the Privacy Act reforms). The proposed close consultation with other agencies is thus strongly endorsed. This includes mechanisms for streamlining reporting, as mentioned concerning Measure 1 above.

Other measures. Measure 5 focusses on data storage but there are other critical issues to be considered including in relation to data processing. For example, the GDPR in the EU requires organisations to implement technical and organisational measures to ensure a level of security appropriate to the risk of *processing* personal data. This includes measures such as encryption. In addition, critical infrastructure data is vulnerable to "harvest now, decrypt later" attacks by adversaries with quantum computing capability. Guidelines should take this risk into account.

Measure 6

Accountability. One important thing to bear in mind in implementing Measure 6 is the importance of clear accountability. This is an area where SoCI currently does not perform well. Generally speaking, SoCI *removes* liability by providing immunity to organisations where harm results from the implementation of a mandated measure. However, it does not currently *impose* liability for such harm on anyone. The consequence is that those harmed may have no recourse. Instead, liability should clearly fall where the fault lies, including on the government where it exercises powers under SoCI. While granting powers to the government in situations such as those outlined in Measure 6 may be important, it is equally critical that those powers be exercised diligently.

Measure 7

Complexity. Our research supports the comment in the paper that the complexity of secrecy law has significant consequences for data sharing. We explored these issues in research conducted some years ago with the Data to Decisions Cooperative Research Centre and are happy to share our findings on the impact of complexity on sharing across law enforcement agencies if that is useful.

Measure 8

Non-endorsement. Measure 8 could be further improved by clarifying in regulatory guidance material that the failure to exercise the proposed power is not an endorsement of the CIRMP, even if submitted. This avoids a scenario where an organisation claims (in litigation or elsewhere) that its risk management processes were in some way approved due the absence of any direction otherwise.

Measure 9

Existing safeguards. While we agree in principle with shifting the telecommunications sector security regime (TSSR) into SoCI, nothing proposed under Measure 9 should operate to weaken or lessen the legislative safeguards that apply to the content of communications, and the access, use and disclosure of communications, information and data as contained in the suite of obligations that already exist in legislation.

Telecommunications is a complex industry regulated by extant privacy, competition, consumer, security, defence and disaster management frameworks, including Part 13 (protection of communications), Part 15 (industry assistance) and Part 16 (defence requirements and disaster plans) of the *Telecommunications Act 1997* (Cth) (TA) and the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA) (warrants and authorisations). The privacy-protecting regimes of the TA and TIA contain strict protections for the content or substance of communications and have distinct requirements relating to the access, use and disclosure of communications, information and data. The existing requirements and processes for securing privacy, and regulating access, and assistance, including thresholds for warrants and authorisations contain notable gaps.[1] However, they must not

[1] See Jake Blight, 'ASIO telecommunications interception and data access powers' (2023) 48(4) *Alternative Law Journal* 288-292

be undermined, or further weakened through the operation of any new or revised powers, responsibilities, or requirements. The relationship of the current regime with new requirements that would come into effect with measure 9 such as incident response and consequence management, will need careful consideration. We note that SoCI contains provisions to protect against warrantless access to the content of communications (see for example. SoCi, Part 3A, Division 3, 35AK(5)).

Transparency. The transparency of the reform process would be enhanced if an unclassified version of the Telecommunications Security References Committee (TSRC) report were published. Too much secrecy is an acknowledged problem of security regulation in democratic countries. Assertions of industry consensus for Measure 9 do not provide enough information about how and where consensus was reached on the proposed major structural change to the telecommunications regulatory framework. Practically, Measure 9 shifts the object of telecommunications sector security regulation from 'telecommunications' to 'critical infrastructure', thereby privileging security over other important telecommunications sector policy goals, such as competition, competitiveness, and responsiveness to consumer interests. The interests of consumers, the privacy of communications, and the ability of the telecommunications sector to compete with local and global businesses across the entire communications sector continue to be pressing policy and regulatory concerns. While there are obvious benefits to a coherent framework for critical infrastructure protection that includes telecommunications, Measure 9 will deepen the regulatory divide between consumer interests, industry competitiveness and sector security. Because the SoCI regime relies on the cooperation of critical infrastructure industries, the views of the affected industry are a key factor in the reform process. Australian citizens, consumers and businesses merit more than a statement in the consultation paper that the 'telecommunications industry' has been consulted on the proposal through the TSRC.

Yours sincerely,

Professor Lyria Bennett Moses FAAL, SMIEEE

Dr Praveen Gauravaram (in his capacity as Adjunct Associate Professor at UNSW)

Scientia Professor Gernot Heiser FTSE FEA ML FACM FIEEE

Professor Sanjay Jha

Dr Susanne Lloyd-Jones

Associate Professor Kayleen Manwaring

Dr Sushmita Ruj, SMACM, SMIEEE