Ramsay
Health Care

14 April 2023

Department of Home Affairs
PO Box 25
Belconnen ACT 2616
Australia

By email: auscyberstrategy@homeaffairs.gov.au

To whom it may concern,

Ramsay Health Care Australia (RHCA) appreciates the opportunity to provide comment on the *2023-2030 Australian Cyber Security Strategy*.

Ramsay Health Care (RHC) provides quality healthcare through a global network of clinical practice, teaching and research. RHC's global network extends across ten countries, with over eleven million admissions and patient visits to facilities in more than 530 locations. RHCA has over 70 private hospitals and day surgery units in Australia and is Australia's largest private hospital operator, employing more than 30,000 people.

Firstly, RHCA **strongly recommends** any reforms must align with the Government's broader policy platform, including the Privacy Act Review, the new National Office for Cyber Security, and the Healthcare Identifiers Act. The Government must ensure its policies align to safeguard a cyber-resilient nation which protects all Australians and provides for a digital environmental that is safe, trusted, and secure.

It is critical that relevant departments (Department of Home Affairs, Attorney-General's Department, Department of Health, Department of Foreign Affairs and Trade) that have overlapping responsibilities work closely together, and with the private sector. This will ensure there is a consistent approach across Government to support Australia to become a world-leader in cyber security by 2030. It is strongly encouraged the Government establishes interdepartmental committees (IDC), at least at the Deputy Secretary level, to progress and ensure the successful implementation of the Strategy.

Secondly, RHCA **recommends** the Government harmonise and simplify existing legislation and regulations (Commonwealth, State, Territory) to ensure there is a consistent approach to cyber security, including related obligations and requirements (such as data disclosure). Streamlining and simplifying regulation in order to promote its effectiveness should be a priority for the Government, rather than introducing additional regulations to an already complex and burdensome system for the private sector.

The Government should consider tasking the Regulatory Reform Division, Department of Finance (formerly the Deregulation Taskforce, Department of the Prime Minister and Cabinet) to undertake this review, given the Division has undertaken similar reviews such as health practitioner regulatory settings, automatic mutual recognition of occupation licences and excise and excise-equivalent goods system.

Thirdly, RHCA **encourages** the Government to provide support to all organisations to uplift capability and capacity in relation to cyber resilience, including to support them to address any additional regulation. This will enhance Australia's overall cyber security ecosystem and the uptake of appropriate cyber security services and technologies whilst supporting Australia's national resilience and economic success.

Lastly, RHCA can bring a global perspective to this conversation given the Ramsay Group has operations across the United Kingdom, European Union, Asia, and Australia. RHCA would be happy to contribute its perspective by participating in the round tables to be held by the Expert Advisory Board and the Global Advisory Panel. It is important the Government takes learnings from overseas, rather than duplicate and rework significant progress which could be implemented within Australia.

RHCA supports a multi-stakeholder system that places individuals, industry, civil society, academia, and government in equal footing ensures responsible and accountable technical management and governance of the internet.

Thank you for the opportunity to provide a submission.

Kind Regards,

[redacted]

Christopher Neal
Group Chief Information Security Officer
14 April 2023

Answers to 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?

Ramsay Health Care Australia (RHCA) **strongly recommends** that the Strategy address the following four key areas to build cyber resilience:

1. Harmonise/simplify legislation and regulations – to ensure there are consistent regulatory obligations across Australia, at both the Commonwealth and State and Territory levels. There is a clear risk that overlapping and complex regulations will reduce compliance levels, create confusion across sectors and undermine the effectiveness of any reforms. For the healthcare sector in particular, it is critical that the relevant regulatory obligations are consistent and work together to drive uplift and support the protection of patient information.
2. Data retention standardisation – to reduce the necessity and permission for organisations who collect from secondary sources (i.e., not direct from a patient) to have more limited / shorter rights of retention, with an explicit goal to minimise the period organisations need to retain personally identifiable information. This would reduce the size of the target for threats, by not duplicating, replicating or sharing personally identifiable information with intermediary organisations, unless necessary.
3. Government clarification and guidance – to clearly outline expectations of organisations through a practical lens of what can realistically be implemented. Such clarification will likely need to be scaled for organisations based on size. For example, what is practical for an ASX listed organisation may not be practical for a small private general practitioner clinic.
4. Government assistance - for all organisations on how to procure services/solutions that are cyber-safe by default and will provide inherent cyber-resilience. This will be of particular benefit to smaller organisations who are unlikely to be able to afford dedicated cyber security professionals.

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

RHCA **recommends** the Government focus on legislative reforms which provide a minimum “floor” for cybersecurity expectations to enhance cyber resilience across the digital economy. These legislative reforms should focus on development of risk management frameworks reflective of an organisation’s individual risk factors, such as size, revenue, sector, or impact to the broader economy.

RHCA also **recommends** developing a national digital identity to be used across both the public and private sector which would reduce the need for organisations to collect and store identity documents. Noting that RHC strongly supports each Australian citizen upholding their individual rights, such as the right of anonymity where lawful and practicable under the *Privacy Act 1988 (Cth)*, that is, the Australian Government should not erode these guarantees and freedoms.

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)?

As mentioned, RHCA **recommends** harmonising and simplifying legislation and regulations, rather than introducing additional regulations to improve mandatory operational cyber security standards across the economy. This exercise must consider both Commonwealth and State and Territory legislation, regulations and cross industry regulation when determining the appropriate mechanism.

The Government may wish to task the Regulatory Reform Division, Department of Finance (formerly the Deregulation Taskforce, Department of the Prime Minister and Cabinet) to undertake this review, given the Division has undertaken similar reviews such as health practitioner regulatory settings, the automatic mutual recognition of occupation licences and the excise and excise-equivalent goods system.

Any new regulations, should they be considered necessary, should be risk-based and developed in close consultation with industry having regard to the implications of the potential additional compliance burden.

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?

RHCA **does not support** further reform to the *Security of Critical Infrastructure Act*.

RHCA **recommends** critical infrastructure should be focused on the foundational physical infrastructure required to ensure the Australian economy can continue to operate. Should the Act broadly deem everything 'critical', then nothing would be critical.

Concerns about 'customer data' and 'systems' may be best addressed via the in-progress review of the *Privacy Act 1988 (Cth)* which RHCA has separately provided commentary on. All organisations will collect, store, and process customer data in some form as the economy continues to digitise.

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

RHCA **does not support** amending the obligations of company directors to address cyber security risks and consequences. The existing obligations as defined in the *Corporations Act 2001 (Cth)* and common law already provide a comprehensive legal framework that obliges directors to effectively oversee the management of cyber risk and build cyber resilience (in the same way as they are required to manage other risks, including emerging risks).

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

RHCA **notes** there may be value in developing a Cyber Security Act if the intention is to provide a single vehicle to outline and streamline Australia's cyber security, resilience, expectations, and obligations. RHCA would not support a new Cyber Security Act that introduces new obligations on organisations without harmonisation of existing cyber obligations to bring them under one regulatory framework.

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?

RHCA **notes** Government monitoring of the regulatory burden on business as a result of legal obligations to cyber security will likely require sector specific approaches and be scaled to the size of the organisation.

As mentioned, RHCA **recommends** there are opportunities to streamline existing obligations and frameworks by harmonising and simplifying the relevant legislation and regulations.

<u>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?
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?</u>

RHCA **does not support** the prohibition of payment of ransoms and extortion demands by cyber criminals. The decision of whether to pay a ransom can be very complex and can have significant consequences, including for third parties (such as patients, in the healthcare context). RHCA believes that it is important for entities to have flexibility in this area so that the appropriateness of payment can be considered on a case by case basis, including having regard to input from Government, regulators and experts at the relevant time.

RHCA **recommends** mandatory confidential reporting to Government for payments made, and the outcome would be a more balance approach.

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

RHCA **notes** the Government’s current position on the payment or non-payment of ransoms is extremely clear.

RHCA **recommends** further clarity on the existing legislative framework may allow organisations to more easily determine if a payment is lawful or may constitute a beach of Australian law.

<u>3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?</u>

RHCA **supports** working with our neighbours (and allies), to build and lift our regional cyber resilience and better respond to cyber incidents. As a global organisation, the Ramsay Group continues to balance differing approaches and requirements across the countries it operates in.

RHCA **suggests** the Government ensures cybersecurity is a standing item (across various forums, including free trade agreements, multilateral discussions, bilateral discussions) to progress initiatives to develop a global standard with likeminded nations. This will also support the work of the Ambassador for Cyber Affairs and Critical Technology.

RHCA **recommends** developing common minimum and standards of cyber security protection.

RHCA also **recommends** considering the expansion of ongoing efforts to limit the ability for cyber criminals to operate without consequence, including a mixture of:

- controls on cryptocurrencies,
- engagement with partner countries to ensure effective legal frameworks are in place to prosecute cyber criminals, and
- joint offensive cyber operations to disrupt cyber criminals' operations

RHCA **notes** the following significant work undertaken by Australia's international partners that could be leveraged, including:

- The United States Food and Drug Administration's guidance (and now enforcement of) on cyber security requirements for connected medical devices
- The United States of America Cyber Security and Infrastructure Security Agency's work on liability for the cyber-safety of software and system manufacturers
- The United Kingdom National Cyber Security Centre's guidance on standards for cyber security and accreditation for organisations – Cyber Essentials and Cyber Essentials+

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

RHCA **notes** Australia was the first country to appoint an Ambassador for Cyber Affairs and Critical Technology.

RHCA **recommends** greater visibility of the work being undertaken by the Ambassador for Cyber Affairs and Critical Technology could provide further opportunities to build, elevate and expand international bilateral and multilateral partnerships. Australian organisations (such as Ramsay Health Care) which operate in multiple geographies could be engaged to support the work of the Ambassador.

As mentioned, RHCA **suggests** the Government ensures cybersecurity is a standing item to progress associated initiatives which supports the work of the Ambassador but also the Government's domestic policy platform.

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?

Refer to Question 4.

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

RHCA **strongly recommends** the Government ensures all Commonwealth Government departments and agencies meet the same cyber security and resilience standards being set for private organisations, to serve as a role model and best practice for other entities.

RHCA **notes** the Governments ongoing emphasis for the private sector to share information. It is crucial the Government also shares information and cannot remain elusive in this space (unless restricted by legislation), particularly when it involves certain actors.

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

RHCA **notes** the Governments ongoing emphasis for the private sector to share information. It is crucial the Government also shares information and cannot remain elusive in this space (unless restricted by legislation), particularly when it involves certain actors.

RHCA **strongly recommends** the Government must timely share information with industry on cyber threats. It appears the Australian Cyber Security Centre's (ACSC) ability to ingest, process and disseminate threat information (detailed technical information) in a timely manner is challenged. There is industry perception information is provided to ACSC, but it not reciprocated, that is, the ACSC does not provide industry information.

RHCA **recommends** ACSC's analysis publications (Annual Threat Report) would benefit by being presented to stakeholders with various levels of technical knowledge, such as specific reports to differentiated stakeholder groups with a focus on actionable steps which could be taken. These include:

- Cyber security professionals,
- Directors and senior management of ASX100 organisations, and
- Owners and managers of small and medium organisations.

RHCA acknowledges the ACSC regular deeper analysis publications (e.g., the Annual Threat Report) which provides high quality analysis.

RHCA **emphasises** the most timely and accurate access to threat information comes from non-Commonwealth sources, such as CISOLens and the Health Information and Analysis Centre (H-ISAC), in particular.

RHCA **notes** it is currently a member/partner of the following bodies:

- The Australian Cyber Security Centre (ACSC)
- The ACSC Joint Cyber Security Centre NSW/ACT Industry Advisory Group
- Health Sector Threat Information Sharing Network (TISN)

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) [and] 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?

RHCA **recommends** an explicit obligation of confidentiality on ASD and ACSC regarding information provided about a cyber incident would improve engagement and remove concerns about sharing information.

RHCA **notes** that it would be beneficial for there to be clarity on how this proposal could be implemented in practice, including having regard to Freedom of Information and regulatory implications.

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?

RHCA **recommends** expanded mandatory reporting (notification) of cyber incidents, including demand or payment of ransoms. This will provide Government with better data to inform the public and improve public understanding of the nature and scale of ransomware and extortion as a cybercrime type.

RHCA **notes** this mandatory reporting must be confidential, at least initially, to allow ASX organisations to appropriately manage their continuous disclosure obligations.

As mentioned, RHCA **recommends** there are opportunities to streamline existing obligations and frameworks by harmonising and simplifying the relevant legislation and regulations.

10. What best practice models are available for automated threat-blocking at scale?

RHCA **recommends** best practice models for automated threat blocking at scale is best undertaken at the telecommunications provider level and as close to the source of the threat as possible.

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

RHCA **strongly recommends** the Government continue to focus on STEM and the associated skills but must also undertake a more tailored approach to uplift cyber skills. Cyber security skills are not isolated to just STEM, with key skills such as analysis and communication best developed through humanities rather than STEM.

RHCA **recommends** the Government consider expanding the number of Commonwealth-supported placements for tertiary qualifications (TAFE, university) to ensure Australia has the necessary cyber skills for the future.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

RHCA **notes** there is no well-defined accreditation option globally for cyber security skills and will not be viable for the next 10-20 years as the field is too young/immature for accreditation.

RHCA **supports** growing Australia's domestic cyber security workforce to overcome the current global shortage. Cyber security should form part of education early in the school curriculum, with an increased focus on adult education and cross skilling to lift the overall number of cyber security professionals in the short term.

RHCA **recommends** the Government consider expanding the number of Commonwealth-supported placements for tertiary qualifications (TAFE, university) to ensure Australia has the necessary cyber skills for the future.

RHCA **urges** the Government to ensure current migration workforce initiatives include cyber security professionals, noting there is a current global shortage.

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

RHCA **recommends** the Government should respond to major cyber incidents to protect Australians by allowing organisations to respond and return to operations without undue regulatory intervention.

Though, should the organisation require, and the Government or agency is able provide it, urgent operational assistance will likely be the best response.

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

RHCA **recommends** a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators. This will allow organisations to notify all impacted regulators, providing a material benefit to allow organisations to focus on incident responses.

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

RHCA **recommends** an effective post-incident review and consequence management model with industry would be one that eases the administrative burden of an incident and encourages information sharing. The Government should facilitate a coordinated approach for the post incident review process which enables information to be shared relatively freely.

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

RHCA **recommends** the Government and industry can work together to improve cyber security best practice knowledge, behaviours, and support victims of cybercrime by clearly articulating what best practice looks like for organisations of different sizes. This in concert with broad multi-vector dissemination of common messaging could uplift the understanding of cyber security best practice across Australia.

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

RHCA **recommends** government assistance should be applicable to all organisations, not only small organisations to manage their cyber security risks to keep their data and their customers' data safe. This includes:

- Education (Refer to Question 12)
- Encouraging telecommunication providers and other managed service providers to build and offer cyber-safe services/solutions to small business (Telstra's "Cleaner Pipes" initiative)

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?

RHCA **recommends** clear government education and guidance, in conjunction with the private sector to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia. In essence, the Government must attract further investment in Australia by removing barriers and red tape.

This would include which services are cyber-safe by design and which would require additional controls or investment to be made cyber-safe. For example, the United States plan to begin labelling of Internet of Things (IoT) devices based on their cyber-safety, analogous to energy rating on appliances or safety ratings on cars.

17. How should we approach future proofing for cyber security technologies out to 2030?

RHCA **recommends** the Government consider a liability framework to ensure suppliers and manufactures of systems are accountable for material cyber security deficiencies in their products. Recently, the United States Cybersecurity and Infrastructure Security Agency (CISA) has reignited this debate.

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?

RHCA **strongly recommends** Commonwealth agencies should ensure smaller/newer cyber security firms are not penalised in the procurements process which would ensure there is a viable path to market. In essence, the Government must attract further investment in Australia by removing barriers and red tape. For example, tax and other incentives to private sector organisations to support such firms may also prove helpful.

RCHA **notes** the AustCyber initiative was providing leadership in this area, however, since being absorbed into the Stone & Chalk organisation, this has become less visible.

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

Refer to Question 17.

RHCA also **recommends** the Strategy should be subject to an annual review and refine as necessary. This will ensure the Strategy remains relevant and implementation is effective, noting 7 years is an eternity in the cyber security space.

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

RHCA **recommends** the Government should measure its impact in uplifting national cyber resilience by:

- The number and duration of significant cyber incidents impacting Australians. This should be stable or, ideally, reduce in both impact and time.
- The share/percentage of the economy spent on cyber security services. This needs to grow from the current relatively low base.

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

Refer to Question 20.