ACS Response to 2023-2030 Cyber Security Strategy Discussion Paper

April 2023

Australian Computer Society Inc. (ACT)
ARBN 160 325 931
National Secretariat
Tower One, 100 Barangaroo Avenue, Sydney NSW 2000
PO Box Q534, Queen Victoria Building, Sydney NSW 1230
T +61 2 9299 3666 | F +61 2 9299 3997
E info@acs.org.au | W www.acs.org.au

To Home Affairs, the Australian Government

ACS response
2023-2030 Cyber Security Strategy Discussion Paper

14th April 2023

Dear Sir or Madam.

Thank you for the opportunity to contribute to this critical issue.

The Australian Computer Society (ACS) is the peak professional association for Australia's information and communications technology sector. We represent over 40,000 members working in all sectors of the economy and in all states and territories across the nation.

The ACS is a charity whose principal object is to promote the development of Australian information and communications technology resources. To further this goal, the ACS works to grow the technology sector while making sure that technology professionals act ethically, responsibly, and in keeping with the best interests of the wider community.

In order to respond to this strategy discussion paper, I have called upon the combined advice of a number of very senior cyber security professionals, who are Fellows of the ACS and who have many years of experience between them. Neither the ACS nor those who have contributed have any conflict of interest, either commercial or otherwise.

The ACS strongly supports the Government's aim of making Australia a world leader in cyber security by 2030 and will be happy to support this aim, both in public and in private.

We realise that this is just the beginning of the process to achieve that ambitious goal and we stand ready to provide an ongoing contribution to this process.

Yours sincerely

N.J.A. Tate

Dr Nick Tate
President, Australian Computer Society

Paper Response

Background context

The ACS accredits virtually all ICT degrees in Australia and many cyber security degrees as well. For a list of accredited degrees, please see below:

https://www.acs.org.au/cpd-education/accredited-courses.html

ACS independently co-ordinates and manages a process of peer group assessment for accreditation of degrees against both a Common Body of Knowledge (CBoK) and the requirements of the Seoul Accord. Adherence to the Seoul Accord enables mutual recognition of accredited ICT/cyber security degrees in the UK, Canada, USA, Japan, Hong Kong, South Korea, Japan, and Mexico.

The ACS also accredits individual professionals in both ICT and cyber security. ACS Certified Professionals (CP) are accredited under the ACS Professional Standards Scheme, which has been certified by the Professional Standards Council. This gives them professional recognition from federal, state and territory governments and allows them to limit their liability to $2million. They are also accredited under the IP3 (International Professional Practice Partnership) which is part of IFIP (International Federation for Information Processing). IFIP is the global umbrella organisation of national professional ICT bodies, initiated by the United Nations Agency UNESCO.

Principles

ACS aims to positively influence the development of the Australian Cyber Security Strategy with these goals in mind. Each of these is expanded in greater detail as part of responses to individual questions.

- An appreciable increase in the effectiveness and efficiency of protection of our society from cyber and technically oriented threats.
- A significant improvement in information sharing between government and industry.
- Improvements in the supply, skills and accreditation of cyber security professionals.
- Enhanced cyber-awareness across organisations and the broader community.
- Greater collaboration with regional and international partners.
- A significant improvement in attention to cyber security issues by boards and organisation leaders.

Q1 What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

The following ideas will enhance and strengthen the strategy and help to deliver a much more secure nation by 2030. Some of these ideas are developed further in answers to subsequent questions.

Education and Skills

To address the serious shortage of cyber security skills government, together with the profession, industry, and education, should develop a comprehensive national cyber security ***education strategy*** that ***starts in all schools*** and continues throughout a person's career. This will help to ensure that Australians are aware of the risks and know how to protect themselves and their businesses from cyber threats.

The cyber security education strategy should incorporate relevant cyber-related skills for a variety of careers. This should also cover public administration, business in general and the industries covered by the Security of Critical Infrastructure (SOCI) Act. It will be difficult to attain the “secure society” objective if cyber education is limited to the IT industry.

Just as workplace safety and ICT awareness training is important for business generally, so now is cyber security awareness training. Government could support an extension of the existing International Computer Driving licence (ICDL) scheme to include more topics in cyber security and encourage business to consider adopting it the scheme.

For more information about ICDL, please see the link below:

https://icdl.org/

Government could work with stakeholders in industry, the professions and education to establish agreed standards for cyber security skills and knowledge in Australia.

Research and Development (R&D) and business support

Government could increase funding for R&D in the cyber security domain, fostering collaboration between academic institutions, research centres, and private sector organisations. This investment would help drive innovation, develop cutting-edge cyber security solutions, and build a strong knowledge base in the country. This would help to ensure that Australia is at the forefront of cyber security innovation and is able to develop new solutions to emerging threats.

Government could also offer financial incentives, such as tax breaks or grants, to businesses that invest in cyber security technologies and services. This will encourage organisations to prioritise cyber security and support the growth of the cyber security industry in Australia.

Another option is a national cyber security framework and certification programme specifically for SMEs and their supply chain that includes guidelines, best practices, and training materials. This would help SMEs and their supply chain to better understand the risks and take appropriate steps to protect themselves against cyber threats.

Government could consider providing support for SMEs by actively monitoring the dark web for potential security breaches and providing swift, adaptable sovereign support for remediation efforts.

Q2

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)?

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?

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

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

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?

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?

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?

Government's strategy should address all forms of data, including both business data and personal data.

It should increase the focus on cyber security in critical infrastructure sectors such as energy, telecommunications, and healthcare. This will help to ensure that these sectors are well-protected from cyber threats and can continue to provide essential services to Australians even in the face of a cyber attack.

Recent events have raised concerns that boards of companies and other organisations are yet to allocate sufficient priority and resources to address cyber security risk. This could be improved by requiring directors and officers to obtain a level of controls assurance that corresponds to the inherent risk level to their organisation and its stakeholders. The inclusion of stakeholders is crucial, so organisations are not narrowly focused on the short-term bottom line.

Directors and officers should face penalties for gross negligence or where the controls are manifestly inadequate.

With respect to ransom payments, it is anticipated that the benefits of outlawing ransom payments would be expected to significantly exceed the impacts. The payment of ransoms or the meeting of other extortion demands should be made illegal with the caveat that a designated regulator could give agreement if there is the potential for loss of life, such as if a hospital is being ransomed.

Government could also classify such costs as not being tax deductible nor coverable by insurance.

Q3 How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

Australia should focus on helping our neighbours in the South Pacific to uplift their cyber capabilities. This can take the form of skills transfer, exercises, capability building and technology investment.

Australia should also reflect new strategic partnerships such as the AUKUS agreement and the technology transfer aspects of that agreement into any cyber security national plan.

These goals can be achieved by:

- Fostering collaboration and information sharing between governments, professional industry bodies and cyber security agencies in the region. This will help to ensure that everyone is aware of the latest threats and can work together to address them.
- Developing joint cyber security exercises and training programmes to test and improve regional cyber resilience. This will help to identify gaps and areas for improvement and ensure that everyone is prepared to respond to a cyber incident.
- Provide technical assistance and support to countries in the region that may have less mature cyber security capabilities. This will help to build capacity and improve overall cyber resilience across the region. This technical assistance could build on the good work in the region that is already undertaken by AusCERT and APNIC.
- Encourage the adoption of internationally recognised cyber security standards and best practices. This will help to ensure that everyone is working from the same playbook and can easily collaborate on cyber security initiatives.
- Develop regional and partner incident response frameworks and protocols to ensure a coordinated response to cyber incidents. This will help to minimise the impact of cyber incidents and ensure a timely and effective response.

This work could build on the establishment of Information Sharing and Analysis Centres (ISACs) in Australia (described below in response to **Q7**).

Q4 What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

Government could consider the following five initiatives to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective:

- Through DFAT and other relevant departments, build stronger cyber security relationships with key international donors and organisations such as the World Bank, the Asian Development Bank (ADB), United Nations, the International Telecommunication Union (ITU), Asia-Pacific Economic Cooperation (APEC) and the Organisation for Economic Co-operation and Development (OECD), ensuring that investments and programmes are aligned. These organisations play a critical role in shaping international cyber security norms and standards and can help to facilitate cyber security cooperation between countries.
- Increase cyber security partnerships with developing countries to build their cyber security capacity and promote cyber security awareness. This will help to create a more secure global digital environment and reduce the risk of cyber threats originating from these countries.
- Provide technical assistance and support to countries in the region that may have less mature cyber security capabilities (as an example the pacific islands). This will help to build capacity and improve overall cyber resilience across the region.

- Strengthen cyber security partnerships with Five Eyes and AUKUS partners to share intelligence and coordinate responses to cyber threats while at the same time developing closer cyber security partnerships with key allies and trading partners such as the European Union and India.
- Deepen cyber security cooperation with key regional partners such as Japan, Singapore, and South Korea. These countries have similar cyber security challenges and can collaborate on initiatives such as threat intelligence sharing, cyber security capacity building, and joint cyber security exercises.

Q5 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?

Government could consider funding some of Australia’s contributions to the international standards community. This activity currently relies on volunteers who either do their analysis as part of a vendor funded position, or by working in their spare time to enhance security standards. This existing approach is unlikely to give Australia key opportunities to enhance international security related standards.

Q6 How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

It is difficult for Commonwealth Government departments and agencies to serve as a model for other entities if they themselves do not set an exemplary example of best practice. In the June 2022 ANAO report, only 2 of 19 entities examined had managed to reach the mandated Policy 10 maturity.

The Government could set an appropriate target level of cyber security practice for each department or agency, publish the target and mandate that it must be achieved by a particular date, with regular monitoring to demonstrate progress.

Q7 What can government do to improve information sharing with industry on cyber threats?

The Government could expand the existing information security sharing frameworks and require business, NFPs, Government agencies and Government Owned Companies (GOCs) to adopt it. Such a framework could allow organisations to confidentially share incident details and root cause analysis, but there would need to be legal protection for organisations sharing incident details.

Experience has shown that trust is a significant consideration for private organisations sharing security information with Government and potentially other industry participants that may be business competitors. Yet, to be effective in combating cyber threats, information does need to be shared between government and industry and between organisations themselves in particular industry sectors.

This can be addressed by using an independent third party that facilitates confidential sharing of data and combined analysis of it. One approach which has been shown to work in the USA is that of Information Sharing and Analysis Centres (ISACs).

ISACs originated in the United States via a presidential order from President Clinton in 1998 (Presidential Decision Directive 63) with the aim of establishing a framework of centres which would share information and analyse threats. They are usually established by industry sector (eg. Finance ISAC, Energy ISAC or Education ISAC) and they are independent, member-driven and established in such a way that both industry and government can trust them.

In the United States ISACs have evolved, and the National Council of ISACs has 26 member organisations covering a wide range of industry sectors. More information about them is available via the link below:

https://www.nationalisacs.org/

ISACs have also gained traction within the European Union (EU) and information about ISACs in the EU, is available via the link below:

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

Another approach to this issue has been that taken by Computer Emergency Response Teams (CERTs) also sometimes called CSIRTS (Computer Security Incident Response Teams). Some of their functions overlap with that of ISACs but they can have greater focus on incident response. They have been around since the 1980s, with AusCERT being a notable example in Australia. More information on the Global Organisation of CERTS/CSIRTs is available via the link below:

https://www.first.org/

For Australia, Government could address the problem of data sharing by encouraging the establishment of ISACs on a scale suitable for this country, and by developing the necessary legislative framework to support them. It would be essential that ISACs are established as independent not-for-profit entities so as to engender trust from all parties.

Q8

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?

It is unclear whether legal confidentiality requirements on government cyber teams will make anything other than a marginal difference for sharing incident information. Organisations are likely to withhold data for hypothetical legal reasons and fears of reputational harm.

Sadly, regardless of legal confidentiality protections, many businesses do not yet appear to have sufficient trust in the security of government systems and processes. This trust deficit is contributed to by the audit findings discussed in the response to **Q6** and by examples both in Australia and overseas where breaches have occurred.

The theft of data from the Office of Personnel Management (OPM) in the USA, where 22 million personal records were affected, is an example of an avoidable data breach, resulting from poor security practices, which contributes to the trust deficit. Further information on the OPM Data Breach is given below:

https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach

It seems likely that the data sharing mechanism, involving ISACs, which is described in the response to **Q7** would be a more effective way to support information sharing.

Q9 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?

Making the regime simple and straightforward to use, together with expanding the scope of incidents to be reported, is likely to improve the quality and quantity of data collected.

However, this would only improve public understanding if it is reported publicly on a reasonably regular basis. There is a danger of cyber fatigue setting in unless someone is directly affected. Unfortunately, there seem to be very limited examples of punishment for cybercrime, and this will not help public understanding of the nature and scale of cybercrime.

Q10 What best practice models are available for automated threat-blocking at scale?

The only practical approach to achieve this is for ISPs to provide this service. Large corporates have the means to implement effective threat blocking on their own, but this is simply not possible for the majority of internet users, including SMEs. The industry code for Carriage Service Providers could be extended to include such a service.

An example of the effective implementation of such a service in Australia can be found in the services provided by the University owned Telecommunications carrier, AARNet. This carrier provides services to all universities and many other cultural and educational institutions and includes a number of cyber security-related services, which can be viewed via the link below:

https://www.aarnet.edu.au/cyber-security

Q11 Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Yes. A cyber resilient Australia cannot not be achieved via the STEM skills agenda alone. It will require a more holistic and targeted response.

There is both a serious shortage of cyber security professionals and a lack of cyber security awareness in other IT professionals, businesses and other organisations. The Government's broader STEM agenda is just too broad to be likely to increase the number of cyber security professionals and does not address the lack of cyber security awareness.

Government could consider the follow initiatives:

- As discussed in the response to **Q1**, Government, together with the profession, industry, and education, should develop a comprehensive national cyber security education strategy that starts in all schools and continues throughout a person's career.
- Encourage all tertiary intuitions providing training in ICT skills to incorporate a minimum level of cyber security skills.
- Consider requiring all immigrants on ICT oriented visas to have a minimum level of cyber security skills.
- Encourage all tertiary intuitions providing business qualifications to cover basic cyber security awareness.

- Consider the development and adoption of an extended International Computer Driving licence (ICDL) scheme covering more topics in cyber security (as discussed in the response to Q1) and encourage high schools to offer this subject.

Q12 What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

This question has been partially answered in the responses to other questions. However, the following initiatives would significantly support Australia's cyber security workforce:

- Consider establishing a programme like the US Government's National Centres of Academic Excellence in Cyber security (NCAE-C) program, which establishes standards for cyber security curriculum and academic excellence. This has proved very effective in the United States in increasing the training of potential cyber security professionals. Further information about this programme can be found via the following link: https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/
- Increase investment in cyber security education and training programmes to provide a pipeline of skilled cyber security professionals. A coordinated approach needs to be established for programmes at school that lead to higher educational pathways. This could include initiatives such as scholarships, internships, and apprenticeships to help students and new graduates enter the cyber security industry.
- Streamline the immigration process for skilled cyber security professionals, who can demonstrate appropriate skills, to address shortages in the domestic market. This could include fast-tracking visa applications and providing incentives for cyber security professionals to relocate to Australia.
- Collaborate with ACS, industry, the profession and academia to develop a cyber security curriculum that is aligned with industry needs and trends. This will help to ensure that students and new graduates are equipped with the skills that are in demand in the cyber security industry.
- Provide incentives for ongoing professional development and training opportunities for cyber security professionals to keep their skills up to date and adapt to changing cyber security threats. This could include initiatives such as mentorship programs, continuing education courses, and attendance at industry conferences and events.

Q13 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?

As discussed in the response to **Q9**, a single reporting portal could help with the more effective reporting of data. However, if the approach of using ISACs for data sharing, which is discussed in the response to **Q7**, were to be adopted then reporting in the first instance for many organisations could be to their sector ISAC. Some aggregation from ISACs might then be needed. In any case, harmonisation of existing reporting requirements would be a considerable improvement on the current position.

Q14 What would an effective post-incident review and consequence management model with industry involve?

An effective model might involve a collaborative approach with industry using the ISAC sharing and analysis model, which was discussed in the response to **Q7**.

Q15 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?

Government could look at cyber security as being similar to workplace health and safety. It is an accepted principle that a safe workplace can only be achieved when all people in an organisation integrate safe work practices. For example, safety in procurement management is as key to safety, as is safety on a workshop floor. Looking at cyber security through this lens could provide the means of disseminating best practice knowledge and behaviours as well as proving some support to the victims of cybercrime.

Government could further support SMEs by seeking to engage them in an ISAC ecosystem, which was discussed in the response to **Q7**.

Cyberisk insurance appears to be increasingly difficult to secure for many businesses, particularly as there appears to be no underwriter in Australia. Government could work with the insurance industry to see if this is becoming a market failure and, if so, what options there might be to address it.

There are a number of services that can automatically look at the externally facing assets of an organisation in order to determine their security posture. Government could consider negotiating with one of more of these service organisations, with potentially some level of subsidy, in order to make them highly attractive for SMEs.

Q16 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?

The response to this question has already been partially covered in the response to **Q1**. However, the initiatives listed below, could help to enhance the ecosystem, and support the uptake of cyber security services and technologies in Australia.

It is difficult for consumers and small business to understand what security measures a technology product (particularly software and its configuration) has implemented, and this makes it hard to make the best choice. Government could consider sponsoring or co-developing a star rating scheme for the security of technology products. This would be analogous to the star rating scheme for the energy consumption of a device.

Government should continue to work with AustCyber in their role as an industry growth centre to ensure that they contribute to future development of Australia's cyber eco-system.

Q17 How should we approach future proofing for cyber security technologies out to 2030?

The answer to this question is partially covered by the response to **Q1**.

Nevertheless, implementing or mandating the use of suitable methodologies in the design of systems such as using the "security by design" approach for system development would significantly help with future proofing and with improved quality. There is still a tendency to trade off security in the race to bring product to market and a good example is in the development of some products in the Augment Reality (AR)/Virtual Reality (VR) arena.

Government might consider an industry Code of Practice for secure software development.

Q18 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?

Yes. Government is a large an important purchaser in the Australian technology market, but that market is still small in global terms. If the default position of Government, particularly for technology and cloud services, is to procure from large global organisations then this will work against local SMEs gaining a viable path to market.

An example of an attempt to support Australian Technology suppliers is the Queensland Government's Buy Queensland policy. More details of which can be viewed via the link below:

https://www.epw.qld.gov.au/about/strategy/buy-qld/about

Q19 How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

The Australian strategy should be based on principles that will stand the test of time, rather than just addressing immediate concerns. Cyber security is an important element of many emerging technologies, such as quantum computing, space, artificial intelligence (AI) and robotics. It is important that these new emerging technologies consider cyber security implications in their design and development phases.

Q20 How should government measure its impact in uplifting national cyber resilience?

Government should develop and implement a measurement framework that broadly tracks national cyber resilience through a range of measures and controls. It is likely that this would require Government to enhance existing reporting regimes through regulation. Measures which might be reported on could include Data and Privacy breaches and cybercrimes reported to relevant authorities.

Q21 What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

It is important to provide objective periodic assessments of progress. In terms of the strategy, it will be important to be able to give yearly updates on what has been achieved and what is outstanding. This should also show the evolution of the strategy as new elements may need to be added in emerging areas.

ENDS