2023 – 2030 AUSTRALIAN CYBER SECURITY STRATEGY

Australian Government

DISCUSSION PAPER

Expert Advisory Board
Andrew Penn AO (Chair)
Air Marshal (ret'd) Mel Hupfeld AO DSC
Rachael Falk

We acknowledge the Traditional Custodians throughout Australia and their continuing connection to land, sea and community. We acknowledge the Ngunnawal people, the Traditional Custodians of the land on which this paper was prepared, and we pay our respects to their Elders, past, present and emerging.

MINISTER'S FOREWORD

Minister's Foreword

As Australia's first Cabinet Minister for Cyber Security I am focused on creating a digital environment that is safe, trusted and secure. As a nation we have a unique opportunity to move cyber security beyond a niche technical field to a strategic national security capability that underpins our future prosperity.

The case for change is clear. Australia has a patchwork of policies, laws and frameworks that are not keeping up with the challenges presented by the digital age. Voluntary measures and poorly executed plans will not get Australia where we need to be to thrive in the contested environment of 2030.

The digital age presents enormous opportunities. To achieve our vision of being the world's most cyber secure country by 2030, we need the unified effort of government, industry and the community. Together, we can equip our community to reduce the number and impact of cyber incidents through improved cyber hygiene and provide clear advice on how to respond confidently when they occur.

This discussion paper is an opportunity to provide your views on how we can work together to make Australia a world-leader in cyber security by 2030. This means:

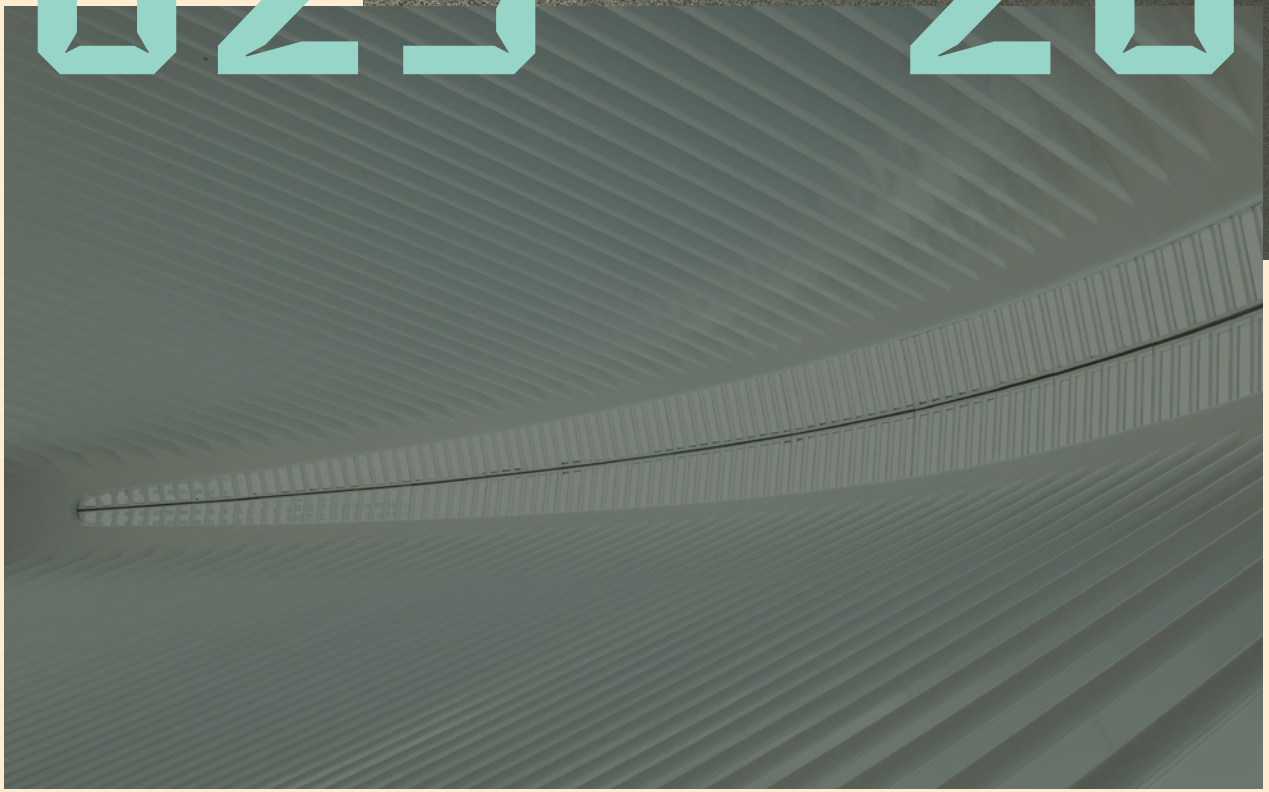
- Australia has a secure economy and thriving cyber ecosystem;
- our critical infrastructure and government systems are resilient and secure;
- we have a sovereign and assured capability to counter cyber threats; and
- Australia is a trusted and influential global cyber leader, working in partnership with our neighbours to lift cyber security and build a cyber resilient region.

I have appointed an Expert Advisory Board to assist and advise the Government on the development of the *2023-2030 Australian Cyber Security Strategy*. The Board is chaired by former Telstra CEO Andrew Penn AO, who is joined by Mel Hupfeld AO DSC and Rachael Falk. The Board is working closely with industry, civil society and academia to advise the Australian Government on the steps we need to take to make Australia the most cyber secure nation in the world by 2030. The Assistant Foreign Minister, the Hon. Tim Watts MP, is also closely involved in the development of the *2023-2030 Australian Cyber Security Strategy*, leading our approach to how Australia can work in partnership with our region to lift our collective cyber security.

Setting Australia up for success in the digital age begins with meaningful engagement and transformative partnerships across all levels of government, industry and the community. To achieve this goal, the Government is developing the *2023-2030 Australian Cyber Security Strategy*, and we want you to be a part of the discussion.

The Hon Clare O'Neil MP
Minister for Home Affairs
Minister for Cyber Security

CYBER 2023 - 2030



Introduction from the Expert Advisory Board

Technology continues to develop at a rapid pace and it is already an integral part of the Australian way of life – it connects our cities, workplaces, schools, and homes. The mobile devices we carry with us every day are super computers in our pockets. Technological advancements have meant that things that once took hours can now be done instantly via a browser, such as checking on our pets at home, shopping 24/7 from the convenience of our homes, and screening visitors at our front doors from thousands of kilometres away.

While this is a discussion paper for the *2023-2030 Australian Cyber Security Strategy* (the 'Strategy'), when we refer to 'cyber' we mean the conduit by which all Australians can engage in a wide range of activity digitally such as shopping, banking, work, education, and healthcare. However, we also note that 'cyber' provides a conduit for crime, foreign interference, espionage, disinformation and misinformation. Cyber security is the means by which the cyber foundations of the digital world are secured. We are seeking your views to inform our recommendations to Government as to what it should consider when developing cyber security measures to better protect and enhance our collective cyber resilience, both in Australia and in the region.

Our national resilience, economic success, and security rely on us getting our cyber settings right. Importantly, 99% of Australians now have access to the internet.[1] During the COVID 19 pandemic, classrooms and workplaces moved entirely online, which contributed to the rapid acceleration of living in a digitally connected world. The adoption of digital technologies by some organisations was sped up by three to seven years in just months.[2]

Uplifting Australia's cyber resilience would also provide a significant boost to the domestic digital economy. The Australian cyber market contributed approximately $2.4 billion in Gross Value Added (GVA) in 2022, and the sector's GVA grew by 11% from 2020 to 2022.[3]

1 www.acma.gov.au/publications/2022-12/report/communications-and-media-australia-how-we-use-internet
2 www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20new%20digital%20edge%20rethinking%20strategy%20for%20the%20postpandemic%20era/the-new-digital-edge-rethinking-strategy-for-the-postpandemic-era.pdf
3 AustCyber Sector Competitiveness Plan (2022)

The CSIRO estimates that Australia's cyber security revenue could reach $6 billion per year in 2026.[4]

The rise in revenues and employment in the cyber security industry also has flow-on benefits for a range of domestic sectors and areas of sovereign capability. Australian businesses rely on cyber security professionals to secure their technologies, protect valuable intellectual property, and ensure that customers can trust Australian technical goods and services. In emerging fields such as quantum technologies, artificial intelligence, biotechnologies, and robotics, cyber security professionals are a vital enabler for the development of assured sovereign capabilities for Australia and our international supply chains.

While this means the world is at our fingertips, there is a darker side to living in a cyber-connected world. Just as Australians have rapidly adopted digital goods, education and services, cyber criminals and nation states have also exploited cyber and the world in which we live. They are highly adaptable, adept, and are readily exploiting vulnerabilities: both software and human.

According to the Australian Cyber Security Centre's (ACSC) 2021-22 Threat Report, one incident is reported on average every 7 minutes[5] with over 76,000 cybercrime reports in 2021-22.[6] Cyber-enabled crimes such as romance and investment scams, business email compromise, ransomware and phishing emails have been successful in stealing identities and money from organisations and hard-working Australians.

Ransomware and associated extortion threats, espionage and fraud have become a significant threat to Australian organisations, large and small. There was no greater example of this than in September and October 2022, when over a three-week period the personal data of over 9.8 million Optus customers and 9.7 million Medibank customers was stolen by cyber criminals. The scale and severity of these breaches meant that cyber security became a topic that is now front and centre in board rooms and living rooms. It became clear during these incidents that government was ill-equipped to respond, and did not have the appropriate frameworks and powers to enable an effective national response given the number of Australians whose personal information, including identity data, was compromised.

While the companies themselves were impacted by these breaches, it is their customers who are the real victims of these insidious crimes. These breaches demonstrate why more needs to be done to make sure our laws recognise there is widespread data collection and government and industry both have an essential role to play in hardening networks and securing our economy. The Strategy must reflect the importance of protecting customer data, and ensure that all organisations have the right cyber security settings in place to make Australia is the most cyber secure nation in the world by 2030. We also need to make sure that we have the right legal and policy settings in place to help break the food chain when it comes to ransomware and related demands from – and payments to – cyber criminals.

All of us must play a role in keeping our critical data, systems and infrastructure safe. From government departments, large organisations, small to medium businesses, academia and society as a whole. This involves not just best practice operational standards, raising awareness about online scams, or ensuring connected devices are secure by design: it means we must also turn our minds to current and future cyber security threats, and work together to do all that we can to protect Australians and our regional partners from these threats.

If we are to lift and sustain cyber resilience and security, it must be an integrated whole-of-nation endeavour. We need a coordinated and concerted effort by governments, individuals, and businesses of all sizes.

4 CSIRO Futures, Cyber Security A Roadmap to enable growth opportunities for Australia (2018)
5 www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022
6 www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

We believe that the development of a new forward-looking Strategy for Australia is a unique opportunity for us to be ambitious and innovative. Any successful strategy must be national in scope, enduring, affordable, achievable, and allow for flexibility to account for changes in the dynamic cyber environment out to 2030.

We appreciate there have been a number of consultations on cyber security and related topics over the last three years, and we will build on this feedback. We also want to make sure that this discussion paper provides you with the opportunity to contribute your views to shape the Australian Government's approach to domestic and international cyber security at this crucial moment as we move into an increasingly online world.

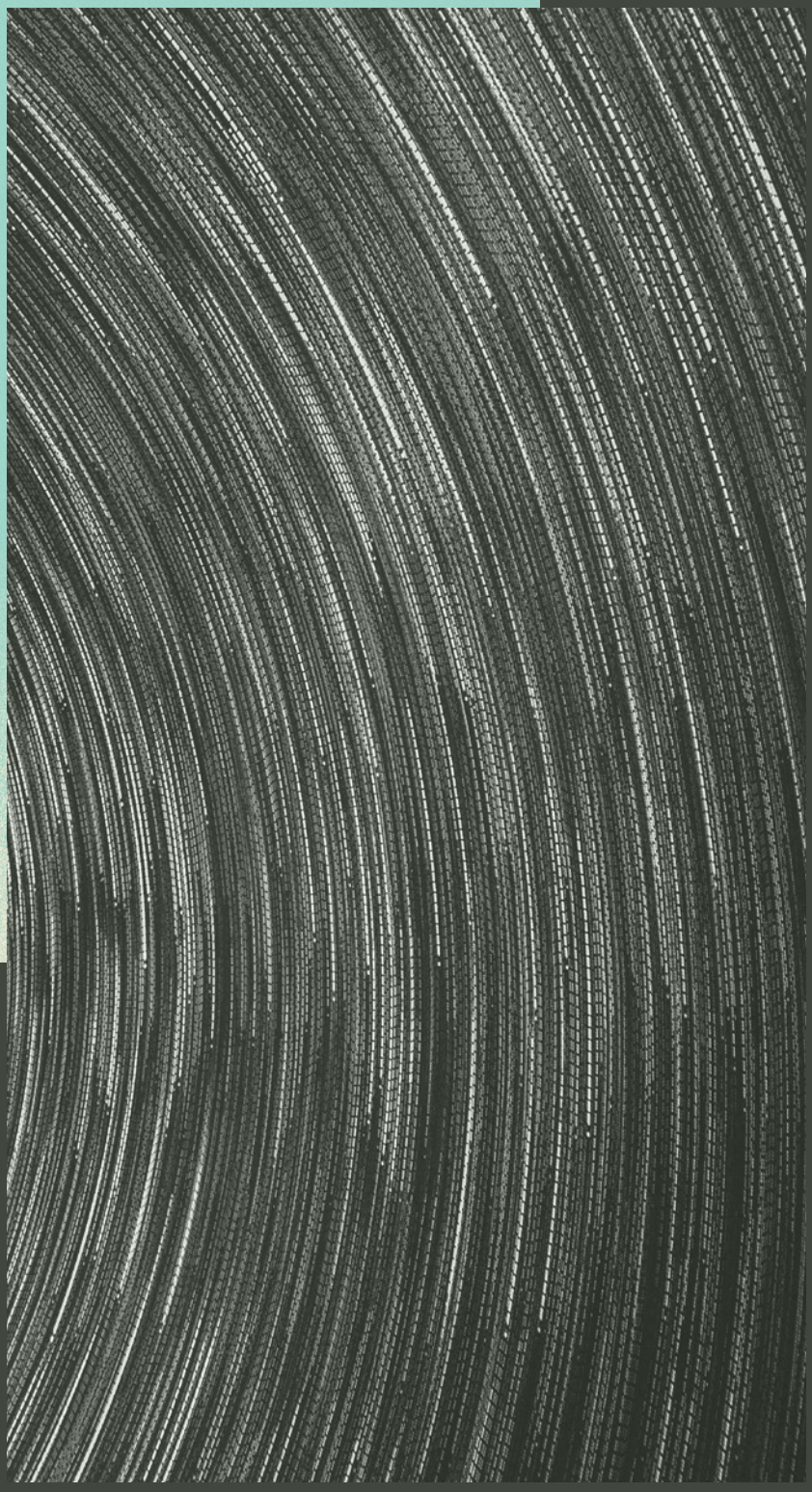
We welcome your ideas and look forward to receiving your submissions.

Andrew Penn AO
Mel Hupfeld AO DSC
Rachael Falk

Andrew Penn AO

Mel Hupfeld AO DSC

Rachael Falk



Australia's Cyber Security Opportunity

The Australian Government's goal of becoming the most cyber secure nation by 2030 is an ambitious aspiration. It recognises that the transition to a digital economy relies on the ability to trust that our personal data, infrastructure, and underpinning systems are secure, even as the cyber threat landscape evolves. Our ambition to become the most cyber secure nation by 2030 can be balanced with our liberal democratic values, and the objective of ensuring Australians can continue to access, engage with, and benefit from the online world.

What would Australia look like as the most cyber secure nation by 2030?

In 2030, every aspect of our lives – social, economic, and cultural – is underpinned by digital connectivity. We live in an increasingly contested and congested cyber environment with state and non-state threat actors, and emergent technologies – like artificial intelligence and quantum computing – shaping the cyber security threat landscape in unpredictable ways. But we have invested in enduring and adaptive sovereign capabilities to build national cyber resilience, which means Australians engage in cyberspace with confidence and assurance.

By 2030, Australia is internationally recognised as a leading brand for cyber goods and services. This means consumers expect advanced cyber security built-in by-design, sold at a reasonable price, designed and manufactured by a workforce with world-leading cyber skills under fair working conditions.

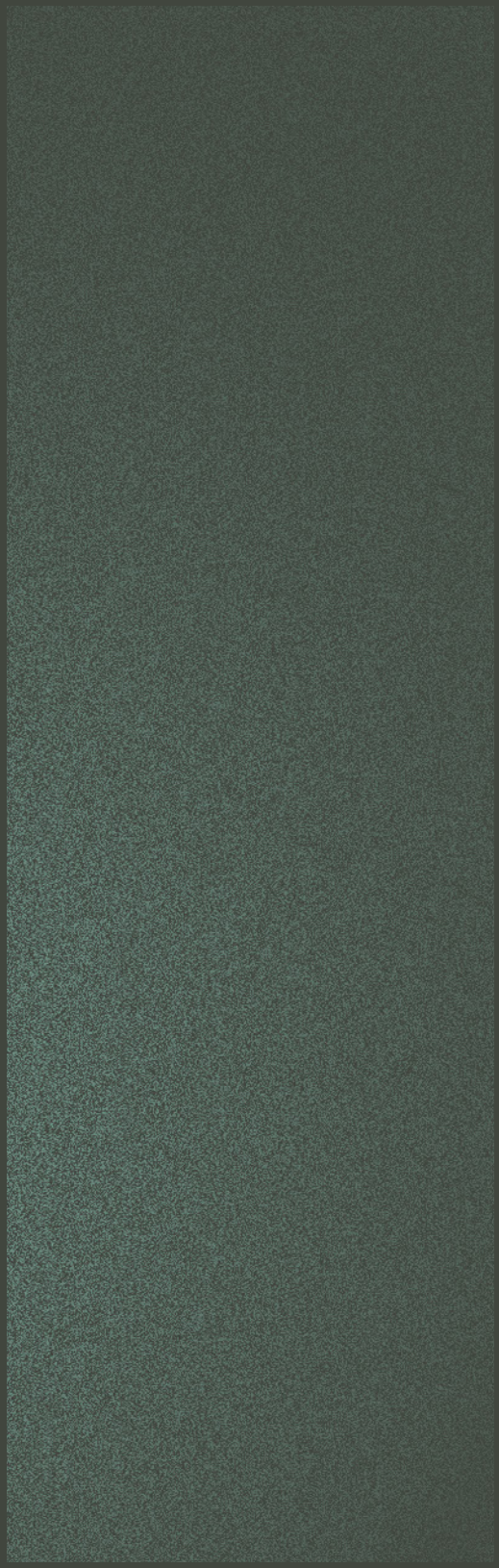
The Australian regulatory system facilitates innovation and stimulates economic growth and recovery. Australian-made products set the international benchmark for cyber services, created in a way that reflects the values of a democratic society; leading on safety and security while respecting basic rights. Customers expect cyber secure technologies in the same way they expect a car to be sold with a seatbelt.

Internationally, Australia is a respected partner, collaborating with and supporting countries in our region and globally to defend the international rules-based order in cyberspace. Australia has built a safe and inclusive online environment, and broader prosperity, upon a strong foundation of cyber resilience in our region. A multi-stakeholder system that places individuals, industry, civil society academia and governments on an equal footing ensures responsible and accountable technical management and governance of the Internet.

With our critical infrastructure increasingly reliant on internet connectivity, Australians have confidence that their access to water, electricity or online banking will not be disrupted because of a cyber incident. While cyber attacks remain prevalent, our continued cyber resilience means we apply learnings from regular scenario planning and testing to ensure we have the right preventative measures in place. When a cyber incident does occur, we have an agile and rapid response to mitigate its harm, recover quickly, and disrupt further malicious acts.

Realising this vision will require that all Australians – regardless of when they were born, where they live, and what language they speak at home – know what practical actions they need to take to keep their personal information, businesses, and families safe online.

This discussion paper represents the start of an ongoing conversation around how the Australian Government can lay the foundations for a cyber secure future, recognising that all Australians have a vital role to play in keeping Australia safe.



Approach to Consultation

The Strategy will be developed in partnership with industry academia, state and territory governments and the Australian and international community. Like Australia's cyber security, the Strategy will be a team effort, building on our history of collaborative cyber resilience.

Australia is uniquely placed to define and adopt world-leading policies in cyber security. Since *Defence 2000: Our Future Defence Force*, Australia has been alert to the need to consider cyber security as a matter of national security.

Australia's Cyber Security Strategy 2016 introduced cyber security as a risk to a broad audience at the foundational level, and *Australia's Cyber Security Strategy 2020* then recommended action across three pillars: governments protecting against sophisticated cyber threats, businesses protecting their customers, and the community making cyber-aware choices.

Australia's Cyber Security Strategy 2020 was complemented by *Australia's 2021 International Cyber and Critical Technology Engagement Strategy*, which set out Australia's vision for a safe, secure and prosperous Australia, Indo-Pacific region and world, enabled by cyberspace and critical technology. Moving forward, domestic and international cyber security policy considerations will be combined into a whole-of-nation effort under the Strategy.

The development of the previous cyber strategies has been followed by consultations on the *Security of Critical Infrastructure Act* (the SOCI Act), the *Strengthening Australia's Cyber Security Regulations and Incentives* discussion paper, and the *National Data Security Action Plan* discussion paper. The Strategy will leverage these consultations and public submissions.

The Expert Advisory Board has commenced consultation on the Strategy through a series of roundtables focussed on the core policy themes identified in this discussion paper. Consultation will continue through to the drafting and publication of the final Strategy before the end of 2023.

The Expert Advisory Board and the Department of Home Affairs will lead consultations on domestic components of the Strategy, and partner with the Department of Foreign Affairs and Trade to lead international-themed consultations to ensure that the Strategy accounts for global perspectives and partnerships.

The Minister for Home Affairs and Cyber Security and the Expert Advisory Board are also being advised on global best practice by a Global Advisory Panel comprising the best minds from our closest allies. The Global Advisory Panel is chaired by Ciaran Martin CB, former CEO of the United Kingdom's National Cyber Security Centre.

SECURITY STRATEGY

The 2023-2030 Australian Cyber Security Strategy

Australia's cyber landscape has evolved significantly since *Australia's Cyber Security Strategy 2020* was released. COVID-19 highlighted our critical dependence on cyber for our productivity, prosperity, and national security as Australians spent more time online than ever before. The Russia-Ukraine conflict demonstrated that cyber attacks by both nation states and criminal groups can rapidly spill across borders and affect critical infrastructure and essential services around the world.[7] The Optus and Medibank incidents also represented two of the most significant data breaches in Australia's history.

Collectively, these events underscore an urgent need to deliver a national cyber security strategy which:

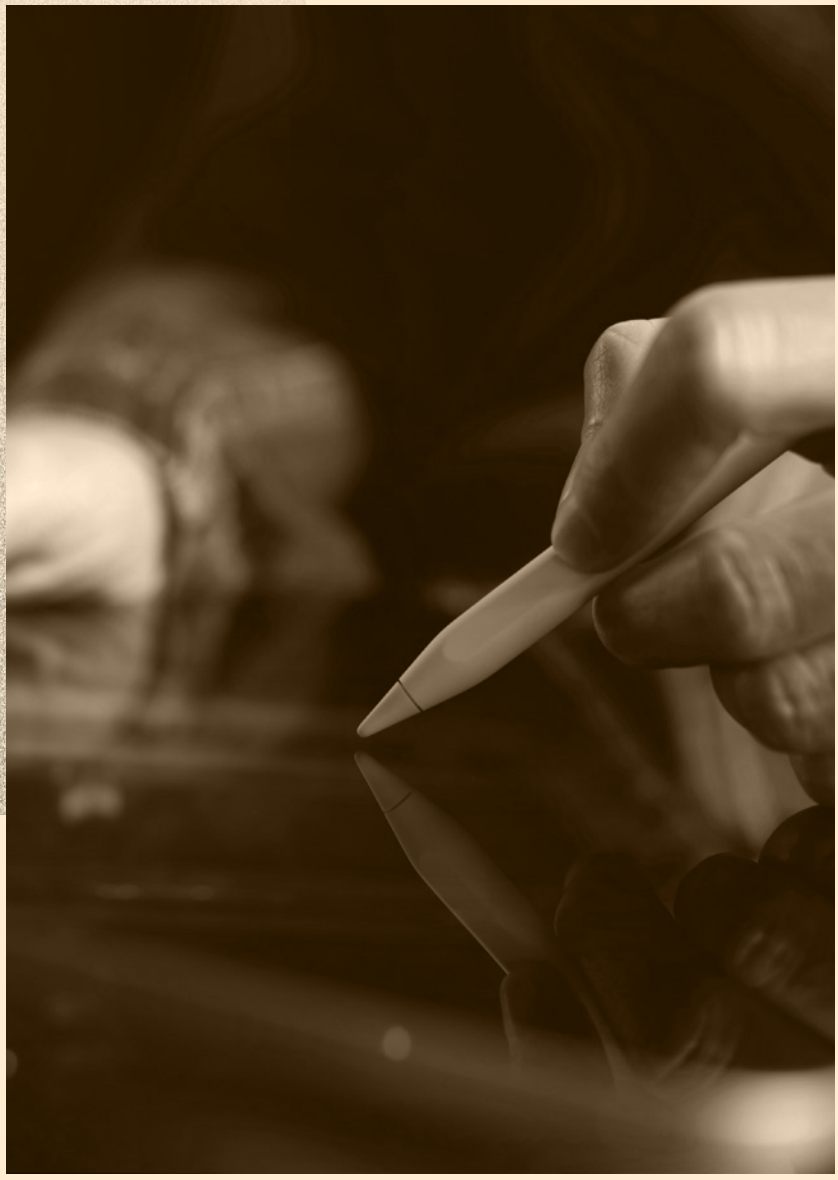
- takes lessons learned from previous stakeholder consultations and major incidents to inform current policy responses;
- sets out the priorities for Australia's cyber security uplift from 2023-2030; and
- seizes opportunities to get ahead of changes in the risk environment, harness new technologies, and position Australia as a global leader on cyber.

There are a range of other important Government priorities which will significantly enhance Australia's digital security and which will progress in parallel with the Strategy. These include:

- the outcomes of the Attorney-General Department's Review of the *Privacy Act 1988*;
- the National Plan to Combat Cybercrime;
- the Australian Competition and Consumer Commission *Digital Platform Services Inquiry 2020–25*;
- Commonwealth Digital ID policy development and reforms;
- measures enhancing the growth of critical technology industries and resilience of supply chains led by the Minister for Industry and Science, including the National Quantum Strategy; and
- investment through the REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers) package administered by the Minister for Defence.

The Privacy Act Review Report was publicly released on 16 February 2023 for consultation on the development of the Government response to the report. Public consultation will remain open until 31 March 2023. The feedback received will also contribute to the development of the Strategy.

7 https://www.cyber.gov.au/acsc/view-all-content/advisories/russian-state-sponsored-and-criminal-cyber-threats-critical-infrastructure



Priorities for the 2023-2030 Australian Cyber Security Strategy

The Minister for Home Affairs and Cyber Security has noted:

"Everyone has skin in the game when it comes to Australia's cyber security. If you use the internet, have a smart device in your home, or have a perspective on what Australia's cyber security should look like, I encourage you to get involved as the Expert Advisory Board seeks views throughout the Strategy's development."

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

This section of the Discussion Paper outlines:

- the core policy areas that the Expert Advisory Board expects will be addressed in the Strategy; and
- a series of potential policy areas, where the Expert Advisory Board is seeking your feedback on what action the Australian Government should take to become the world's most cyber secure nation in the world by 2030.

Core policy areas to be included in the 2023-2030 Australian Cyber Security Strategy

Enhancing and harmonising regulatory frameworks

We have heard from industry that business owners often do not feel their cyber security obligations are clear or easy to follow, both from an operational perspective and as company directors. There are a range of implicit cyber security obligations placed on Australian businesses and non-government entities, including through the corporations, consumer, critical infrastructure, and privacy legislative and regulatory frameworks. However, it is clear from stakeholder feedback and the increasing frequency and severity of major cyber incidents, that more explicit specification of obligations, including some form of best practice cyber security standards, is required across the economy to increase our national cyber resilience and keep Australians and their data safe.

To be the most cyber secure nation in the world by 2030, Australians should have confidence that digital products and services sold are fit for purpose and include appropriate best practice cyber security protections.

There may also be opportunities to simplify and streamline existing regulatory frameworks. For example, stakeholders have encouraged government to streamline reporting obligations and response requirements following a major cyber incident.

It is clear that a package of regulatory reform is necessary. How this would be implemented, including the potential consideration of a new *Cyber Security Act*, drawing together cyber-specific legislative obligations and standards across industry and government, and the details of these reforms is something on which feedback will be welcomed. This should also consider whether further developments to the SOCI Act are warranted, such as including customer data and 'systems' in the definition of critical assets to ensure the powers afforded to government under the SOCI Act extend to major data breaches such as those experienced by Medibank and Optus, not just operational disruptions.

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

See further questions at Attachment A.

Strengthening Australia's international strategy on cyber security

Combined with domestic uplift, strengthened international leadership will enable us to seize opportunities and address the challenges presented by the shifting cyber environment. Australia is a respected voice in addressing the challenge of making the world a safer place online. We can leverage this voice through tangible steps to shape global thinking, particularly in relation to new and emerging technologies.

Cyber resilience is also essential to unlocking economic opportunity and prosperity in our region. Investments in areas such as health, infrastructure, and education are not secure if they are not underpinned by effective cyber security.

Assistant Minister for Foreign Affairs, the Hon. Tim Watts MP, has noted:

"This is not a challenge we face alone. We all – Australia, our region and the global community – benefit from a stable and resilient cyber space. Indeed, without cyber security other gains are too easily lost.

Whether it's developing international cyber space laws and norms, holding accountable those that flout the rules, working to lift regional cyber resilience or leveraging our humanitarian response track record to respond to severe cyber attacks, working with partners is essential to a prosperous and secure cyber environment."

There are three sets of opportunities to explore through consultation on the 2023-2030 Australian Cyber Security Strategy:

1. How Australia can elevate the existing level of engagement with international partners through concrete steps to promote cyber resilience?
2. What opportunities are there to better support the development of international technology standards, particularly in relation to cyber security?
3. How can government and industry partner to uplift cyber resilience and secure access to the digital economy, especially in Southeast Asia and the Pacific?

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

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

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?

Securing government systems

The Commonwealth Government controls and processes some of Australia's most sensitive data to deliver essential public services. Australia continues to be the target of persistent cybercrime and espionage by a wide range of criminal and state actors, including foreign intelligence services, seeking information on political, diplomatic, military, and personal data.[8]

Government should stand as an exemplar of cyber security; however the *Commonwealth Cyber Security Posture in 2022* report (the Cyber Posture Report) reveals government agencies have a long way to go to properly secure government systems. Only 11% of entities in the Cyber Posture Report reached Overall Maturity Level 2 through the implementation of Essential Eight controls, and the majority of entities are yet to implement basic policies and procedures.

Public sector cyber security is comprised of both non-technical and technical elements, and it is crucial to consider both when considering how to better secure government systems. Non-technical aspects include things like governance frameworks and accountability mechanisms, cyber security culture, and risk management planning. Technical aspects include elements such as inventory management and legacy systems, variation across government systems and attack surfaces, and the nature of essential services delivered by each entity.

While acknowledging the work done under previous strategies, these have not achieved the level of progress required to meet the Government's vision. Leadership and accountability are critical at all levels and in all organisations to deliver the Strategy. Enhancing government cyber posture will require a framework which accounts for:

- best practice standards, evaluation, transparency, reporting, and aligned incentives; and
- the appropriate support, accountability and leadership for individual government departments and agencies to manage their cyber security risk profile.

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

Areas for Potential Action by 2030

In addition to the core policy areas, where it is clear interventions will be addressed in the Strategy, there are a range of other areas where potential policy options to enhance cyber resilience could be considered in the Strategy. We are seeking views to inform advice to Government on the following potential areas for policy action:

Improving public-private mechanisms for cyber threat sharing and blocking

There is a broad spectrum of options available to enhance cyber security threat sharing and blocking through public-private partnerships. This requires analysis of feasible technical approaches, which can be deployed sustainably at scale. However, improved threat sharing should also consider qualitative issues, such as government practice related to information sharing, access, declassification of intelligence, and existing regulatory frameworks such as the Privacy Act and the *Surveillance Legislation Amendment (Identify and Disrupt) Act*. There are a range of international approaches which Australia could also consider through the Strategy, recognising these would require further consultation to assess.

8 www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

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

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

See further questions at Attachment A.

Supporting Australia's cyber security workforce and skills pipeline

There is no one single silver bullet for addressing the shortage of skilled cyber security professionals in Australia. Rather, it requires a suite of practical actions conducted under a clear strategy. The Australian Government is pursuing a broad agenda related to science, technology, engineering, and mathematics (STEM) skills, which will support the growth of our future workforce, including in cyber security. More broadly, the Government has committed to reaching 1.2 million tech jobs by 2030. To the extent that cyber security is embedded in STEM curricula, this agenda will improve the available pool of cyber security professionals. However, it is not yet clear whether this will be sufficient for more specialised cyber security career pathways. The purpose of the discussion paper is to determine whether there are additional steps, specific to the cyber workforce, which should be pursued through the Strategy.

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

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

National frameworks to respond to major cyber incidents

It is clear that Australians expect the Commonwealth Government to play a role in responding to major cyber incidents. We need to clarify what the community and victims of a cyber attack can expect from the Government following an incident in the context of victim support and post-incident response. Government must ensure that frameworks for incident management and coordination are fit-for-purpose, and conduct post-incident review and consequence management following major cyber incidents. It is also clear that government should share the root cause findings from investigations of major cyber incidents so that we can all benefit from these learnings. There are a range of international models which serve as useful comparisons, and the Optus and Medibank incidents exposed the gaps in Australia's existing incident response functions. The Strategy provides a mechanism to improve the manner in which Australia responds to major cyber incidents.

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

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

Community awareness and victim support

Despite widespread awareness of the potential risks posed by cybercrime, there is no consistent understanding of the practical steps that consumers, small and medium-sized enterprises (SMEs), and other organisations must take to enhance their cyber security. There is an opportunity through the Strategy to invest further in community awareness and skills building for cyber security, including for SMEs. As with crimes which have devastating impacts on individuals, businesses, and communities, there is scope for Government to explore opportunities to increase support available to victims of cybercrime. While preventing cyber incidents is important, it is inevitable that major attacks will continue to occur through to 2030 and beyond, and Australia should assess its overall cyber posture by viewing remediation and victim support as a key measure of security.

How can Government and industry work to improve cyber security best practice knowledge and behaviours and support victims of cybercrime?

Investing in the cyber security ecosystem

Protective cyber security technologies have been identified as a critical technology by the Government, and cyber security is essential to the secure development and implementation of a broad range of other critical technologies. To become the most cyber secure nation by 2030, Australia must create an environment that attracts investment in cyber security and other critical technologies.[9] There are a range of potential measures which could be explored to promote trade and investment in this space, with clear opportunities for collaboration between federal, state, and territory governments.

9 Australian Government, Critical Technologies Policy Coordination Office, https://storage.googleapis.com/converlens-au-industry/industry/p/prj213f6fb4eef13398228aa/public_assets/Critical-Technology-Profiles.pdf

What opportunities are available for Government to enhance Australia's domestic cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

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

Are there opportunities for Government to better use procurement as a lever to support the Australian cyber security technologies ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

Designing and sustaining security in new technologies

There are a number of emerging technologies, such as quantum, communications technologies, the Internet of Things, and artificial intelligence which will significantly impact, and be impacted by, cyber security. Some of these technologies exist now. Others will rapidly develop from 2023 to 2030 and will disrupt the existing landscape of cyber security. The Strategy must be adaptable to account for changes in the strategic and technological environment in the coming years.

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

Implementation governance and ongoing evaluation

The Strategy will form the foundation of an evolving approach to cyber security into the future. Implementation will require strong governance and a transparent, meaningful evaluation framework to ensure the Australian Government's vision is realised, and the Strategy is fit-for-purpose now and into the future.

How should Government measure its impact in uplifting national cyber resilience?

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

Next steps

We welcome responses to the questions outlined in this Discussion Paper (consolidated at Attachment A) and any additional matters relevant to the Strategy by 15 April 2023.

Responses should be emailed to:
auscyberstrategy@homeaffairs.gov.au

Attachment A: Cyber Security Strategy Discussion Paper Questions

This attachment consolidates the questions for consultation in the *2023-2030 Australian Cyber Security Strategy Discussion Paper* and includes further specific detail.

Respondents may make a submission regarding the entire discussion paper and full list of questions, or select only those questions which are most relevant.

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?
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)?
    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?
        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?
    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?
3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?
4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?
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?
6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

7. What can government do to improve information sharing with industry on cyber threats?
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?
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?
10. What best practice models are available for automated threat-blocking at scale?
11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?
12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?
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?
14. What would an effective post-incident review and consequence management model with industry involve?
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?
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?
17. How should we approach future proofing for cyber security technologies out to 2030?
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?
19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?
20. How should government measure its impact in uplifting national cyber resilience?
21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

Please provide responses to **auscyberstrategy@homeaffairs.gov.au** by COB 15 April 2023.

Australian Government