ACT Government

ACT Government Submission 2023-2030 Australian Cyber Security Strategy Discussion Paper Response

Australia's 2023-2030 National Cyber Security Strategy – Discussion Paper

Australian Capital Territory Government Submission

Introduction

This ACT Government submission details the ACT's recommendations towards the goal of making Australia the most cyber secure nation by 2030 through a revised National Cyber Security Strategy (the National Strategy).

The past few years have seen drastic increases in cyber threat actor activity from all sectors, along with a rapidly changing threat environment characterised by persistent baseline attack vectors and punctuated by 'zero-day' attacks that threaten to—and in some cases do—cause intense, immediate harm with long lasting impacts.

Of the well-known challenges in cyber security, one is paramount: the majority of organisations and individuals do not have the skills, technology, and resources (financial or otherwise) to adequately protect themselves and their stakeholders. A succinct summary of this issue comes from the recently released U.S. National Cybersecurity Strategy:

"Today, end users bear too great a burden for mitigating cyber risks. Individuals, small businesses, state and local governments, and infrastructure operators have limited resources and competing priorities, yet these actors' choices can have a significant impact on our national cybersecurity. A single person's momentary lapse in judgment [sic], use of an outdated password, or errant click on a suspicious link should not have national security consequences. Our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations [sic] and individual citizens."[1]

We agree with this characterisation and consider the following to be government's responsibilities regarding a nation's cyber resilience:

- Protecting its own systems
- Ensuring private entities—particularly critical infrastructure—protect their systems, and
- Engaging in the core business of government such as diplomacy, intelligence collection and use, offensive cyber actions, economic responses to threat actors etc.
- Setting and ensuring compliance with national cyber resilience policy, legislation, and regulatory frameworks.

Recognition of this fundamental issue begs the question of how we address it. No single agreement, project, or body of work can adequately do so. This requires a concerted, holistic, and collaborative effort from the most capable actors, notably government and industry.

To this end, this submission identifies what ACT Government believes the National Strategy should include to address this fundamental issue, within the scope of government's role in national cyber resilience.

[1] National Cybersecurity Strategy 2023

Pain points

We have identified issues that impact our cyber resilience and challenge our ability to improve. While not all can be addressed by the National Strategy, we believe some can be directly influenced while others can be indirectly improved by our recommendations. We note that these are not the only issues ACT Government—or other organisations—face, but strongly believe these are significant issues that the National Strategy must address to improve Australia's national cyber resilience.

The global cyber security skills shortage

A well-established difficulty for most government organisations—particularly non-Commonwealth governments—is the lack of skilled professionals in the job market.[22] Skilled staff are critical for any organisation to build and maintain cyber resilience. From a public sector perspective, ACT Government has experienced first-hand the difficulty the sector has with attracting and retaining personnel. The private sector can simply offer more attractive remuneration packages alongside strong benefits. While remuneration is not the only reason people choose to work with an organisation, in an industry as stressful as cyber security, such packages provide a compelling incentive. Notably—though the impact on the public sector is greater due to resource constraints—this challenge also impacts the private sector, which we have seen evidenced in reduced levels of competition and increasing costs in procurement and timeliness for engagement.

Financial resourcing

Tied to the global skills shortage is the lack of resourcing available to many public sector organisations, particularly non-Commonwealth entities. The lack of financial resources doesn't just impact staffing; it also impacts what uplift is possible and in what timeframes. A risk-based approach to cyber security requires constant consideration of value propositions, and the more limited an organisation's resources, the greater those value propositions must be to warrant funding.

Addressing cyber security resilience through increased legislative requirements will greatly exacerbate this issue for most public sector entities and businesses and must be approached with exceptional caution.

Lifecycle management issues

Tied to both staffing and financial resource concerns is lifecycle management. Appropriate management of a system requires expert input from conception to decommissioning. Poorly designed systems result in heightened security risks, and often become legacy systems as their end-of-life is poorly planned or not considered until it is too late to manage proactively. Proper design and lifecycle management necessitates skilled staffing across the entire duration of a system, as well as the resourcing to support this staffing, and ensure the system is properly maintained. The pressures on staffing and finances for public sector entities compound to create additional pressures for these entities in managing their systems.

Collaboration is key

It's important to note that the above pain points are not unique to ACT Government. In our ongoing cyber security collaboration with the Commonwealth and other jurisdictional governments, we have heard the same concerns about their own cyber resilience. We've also—understandably—heard about similar concerns for local governments for whom the challenges are even greater as they must provide vital community services with an even smaller pool of resources to address cyber security.

Despite these pain points, we must recognise that the responsibilities of government still apply to non-Commonwealth governments. We must also consider our unique powers around regulation, policy, and

[2] The Commonwealth Cyber Security Posture in 2020 | Cyber.gov.au; ASD REDSPICE Blueprint

legislation; in this way, we are some of the 'most capable actors' when it comes to cyber security and must use our powers accordingly.

To this end, we emphasise the critical importance of collaboration, not only in the development of the National Strategy, but in a holistic approach to Australia's cyber resilience across all levels of government, the community, and industry. The National Strategy must be established with collaboration as its baseline, and this can only be achieved through co-design and co-development with stakeholders. Crucially, this co-design and co-development must go beyond simply input to a discussion paper; this is only a starting point. It requires regular, ongoing consultation with numerous opportunities for input as the strategy is developed and should be followed up with at least annual consultation on the efficacy of the National Strategy and its implementation.

Great ambition requires significant investment and intervention

We have already noted the resource challenges we face when aiming to improve our cyber resilience. Indeed, this is a regular theme throughout our submission, and we expect our non-Commonwealth government colleagues to say the same. We support the grand ambition of the National Strategy, and the goal of making Australia one of the most cyber secure nations. However, we must emphasise that such ambition comes at great expense; an expense that—should we fail to meet it—will result in failure.

The success of the National Strategy and its goals hinge on the ability of the Commonwealth government to provide substantial resource investment at a variety of levels. Our intelligence agencies have reported the increasing threat of foreign interference. 'Cyber space' is a rapidly growing, omnipresent theatre of both conflict and projection of power by state actors. Successful cyber attacks by non-state actors can impact nations in complex ways and at scales they have never been capable of before. We have used significant investment to build and maintain our defence capabilities in the physical realm for the protection of our nation and our allies; we must also do so in the digital realm.

Inclusions in the National Strategy

Sovereign Capability / Building a cyber capable workforce

The discussion paper requests consideration of sovereign capability in cyber security, and separately requests consideration of how Australia can build its cyber security workforce. ACT Government considers Australia's cyber security workforce an inherent part of any sovereign capability. We also note that the cyber security skills and awareness of workers outside the cyber security discipline are of crucial importance to building strong sovereign capability and a cyber capable workforce.

A strong local cyber security industry is a high value proposition for Australia, particularly given issues such as the transfer of information outside Australian jurisdiction and the boost it brings to our local and national economies. However, offerings from international and global cyber security firms, software developers, engineers etc. will always have a significant place within our market. Further, bringing Australia's sovereign capability up to the level that it can compete in the market with these international forces suffers from the fundamental issue of an industry shortage of skilled personnel.

The skills shortage is a well-known, global issue, noted by the Australian Cyber Security Centre[3] as a primary reason behind inability of organisations to meet the Essential Eight, and a notable reason that the Australian Signals Directorate is seeking to recruit 1,900 personnel under its REDSPICE initiative.[4]

[3] ASD REDSPICE Blueprint;
[4] ASD REDSPICE Blueprint

The shortage of skilled personnel is exacerbated for government organisations by resourcing constraints. Governments at all levels have exceptional difficulty retaining personnel as private sector organisations can offer far more substantial financial incentives and benefits. We have repeatedly heard these concerns raised during consultations with other state and territory governments and have been subject to them ourselves. This issue impacts private organisations as well, reflected in the quality of competition presented to us through industry engagement.

In addressing sovereign capability, the National Strategy must address the cyber skills shortage. By building a strong, sustainable ecosystem of skilled cyber personnel, the institutes to train them, and the industries, government and private, to provide them with experience to hone their skills. Australia will position itself as a global leader in cyber security talent, which we can leverage towards the goal of being one of the most cyber secure nations.

To address this capability gap as soon as possible, the Commonwealth should:

- consider that cyber security is an essential facet of the business industry, not just the technology industry
- implement a campaign to make a career in cyber an attractive proposition for young Australians
- establish a program of subsidies for tertiary cyber security courses
- engage industry and education providers on reforms to the National Curriculum that will give current and future students the skills needed to best protect themselves and their own personal information, and promote and encourage cyber security as an industry, and
- work with jurisdictional and local governments to establish pipelines that will feed graduates and current trainees of tertiary cyber security courses into public sector positions.
- include in the National Strategy a cross-skilling program between Commonwealth and non-Commonwealth governments to upskill existing staff and help address the skill shortage.

In addition to having an appropriately skilled and sustainable workforce, this would also address difficulties related to security clearances, by creating a pool of eligible cyber security workers. Currently, ACT Government (and other jurisdictions) are unable to security vet staff to appropriate clearance levels, as we must regularly hire non-citizens who are ineligible for Australian government security clearances. To implement some level of clearance, we have established our own security vetting process but do not have access to the same verification assessments available to the Commonwealth. We consider this a necessary step to mitigate security risks, but believe it is an unsustainable model, and comes with its own inherent risks that could be mitigated should we be able to hire staff eligible for Australian Government clearances. We also recommend the Commonwealth Government provide guidance on alternative security vetting processes, to address these needs while Australia builds a security-clearance eligible workforce.

Finally, the expansion of a skilled and security-clearance-eligible cyber security workforce must be supported by national increases in the population's cyber security awareness. The stronger our population's awareness, the fewer successful attacks they—and the system's they use—will experience, and the less impactful these successful attacks will be. However, this will be a time-consuming, ongoing process, and should occur concurrently with the building of greater cyber security awareness. In doing so, we can mitigate risks related to poor cyber security culture while we work towards a state where individual lapses in security posture do not have devastating consequences.

Identity and digital identity - the ecosystem as critical infrastructure

Government services continue to move to digital platforms to better serve their communities. Community members want easy access to these digital services. Identity verification, and ongoing connection to the community through online interactions, is a critical enabler of service delivery. This may require users to relinquish large amounts of personal information in exchange for access to the service, and they should be confident that this information will be safeguarded appropriately.

As shown by the 2022 Optus and Medibank cyber-attacks, customer identity information is a valuable target for cyber criminals. After breaches involving identity information citizens can suffer significant harms including loss of confidentiality through to identity theft, and all levels of current government incur the burden of remediation. While sectors involved in these attacks may be covered by the *Security of Critical Infrastructure Act 2018* (*SOCIA*; Cth) the current regulations for identity proofing, verification, storage, and reuse of this information are ineffective.

Given the change in threat landscape globally since the beginning of the COVID pandemic this information will continue to retain its value and the systems managing it will face an increased risk of attack. To support Australia becoming one of the most cyber secure nations, we need stronger regulation and expansion of the *SOCIA* to include key parts of Australia's identity ecosystem.
These include but are not limited to;

- Identity providers (those systems that manage user identity verification)
- Attribute, credential and relationship providers
- Sources of truth for documentation used to verify an identity e.g (Document verification System, Facial Verification System, State/Territory based licences, and Births, Deaths and Marriage registries).
- Digital signature systems that may integrate with identity providers to support message and signature authentication and integrity for verified users.

These critical systems manage and maintain the integrity of Australians' identity information and access to digital services; as such they must be covered under the *SOCIA* as Critical Infrastructure (CI) assets and Systems of National Significance (SoNS). Given the increased risk of identity fraud related cyber-attacks, these systems also require additional, mandatory security controls based on their use and risk profile. Identifying these systems as CI assets and SoNS will be an excellent first step by requiring them to meet risk management program requirements of the *SOCIA*.

- Australia has developed a sophisticated framework over several years for how digital identity can be managed in the form of the Trusted Digital Identity Framework (TDIF). This public-private sector framework provides guidelines for interoperability, fraud management for digital identity, security, privacy, and accessibility.[5] The TDIF requirements for identity providers include constraints on the use, management, and storage of identity documentation and biometric information once a user goes through the process to verify their identity.
- The TDIF needs to explicitly enable appropriate consent and sharing of information across all governments to correctly establish and protect the identity information of people in the community.

Identity and Digital Identity should support customers having easy access to services, while still ensuring public and private service providers can meet their regulatory requirements. Government—as the provider of identity documentation and other identifiers used by the Australian population—can also provide digital identity services that integrate with federal, state, territory and local government services, and private sector services.

In addition to the CI requirements, federal legislation should also support additional guardrails for identity service providers around security, privacy, incident response, victim support, useability, and access to services, as well as mandatory real-time digital identity fraud identification and management support.

[5] TDIF 02 Overview

Furthermore, the ACT recommends:

- The Australian Government introduce legislation to prevent organisations from unnecessarily storing personal identity information (such as drivers' licences) in their own databases, which could then be subject to unauthorised and uncontrolled publication (cyber-attack) and applying penalties to those found to be non-compliant.

myGov and myGovID

The Commonwealth Government's digital identity services, myGov and myGovID have increased significance due to the sensitive information and critical services they provide.

The myGov audit report identifies 10 recommendations to improve myGov, myGovID and the Australian digital Identity ecosystem. These recommendations have a focus on security, privacy, and safety of Australia's national digital identity ecosystem immediately and into the future[6]. These recommendations also look to make this a truly national service, partnering with states and territories to improve myGovID's reach and throughput amongst the jurisdictions. As identified in the myGov audit, while the TDIF framework supports inclusion for users, the current ecosystem doesn't support a wide range of documentation which limits access for many users.[7] ACT Government recommends using the TDIF as a baseline for documentation supported but taking a collaborative and codesign approach to work towards a comprehensive system of verifiable proof of Identity digital credentials.

We note our recommendations on digital identity from our June 2022 submission to the *National Data Security Action Plan* (*NDSAP*) discussion paper. In our submission we:

- identify the opportunity the NDSAP provides to join up identity systems in Australia to improve integrity and protections of Australians' identity information
- highlight the criticality of the integrity of identity creation and proof of identity processes
- propose evolving identity capabilities to reduce the number of times people must provide their identity information through data sharing between trusted parties
- recommend consideration of how Australia moves from checking identity at a point in time to monitoring digital identity in use.

We reiterate our position on digital identity in the current submission and believe our input to the *NDSAP* submission reinforces our recommendations for the National Strategy.

Based on the importance of Digital Identity to our national cyber posture, the ACT government recommends:

- The National Strategy include development of a National Identity Framework that incorporates the TDIF and collaboration between states, the Commonwealth and private sector. The framework should include:
    - Support for interoperability of Identity models as ways for users to access services including integration requirements for identity provider, relying parties and other ecosystem participants,
    - Verification under a National Identity framework must support the identification of all people who would use the system by allowing for a diverse range of evidence. The TDIF supported evidence can be considered a starting point, but it must go further if we are to ensure we are inclusive in the design of our digital services.

[6] myGov Audit Volume 1: Findings and Recommendations
[7] myGov Audit Volume 2: Detailed Analysis

    - Ensure security, privacy, digital identity real-time fraud management, and interoperability (it needs to integrate with our services, but also support identity providers people may need to use; this differs from the models of ID verification) are embedded from design,
    - Review controls including, integration requirements, policy, security, and other relevant measures for digital signature systems that may integrate with the Australian digital identity ecosystem,
    - Ensure that any user whose identity has been compromised has quick, easy access to remediation via a one government organisation or "no wrong door" approach for identity remediation.
- Ensure the recommended National Identity framework and underlying guidelines for Identity verification, privacy, security, and fraud management are support by legislation. This should also ensure additional controls for this category of CI.
- The National Identity framework must include methods to prevent, identify, and manage digital identity fraud in real-time, and support victims of identity fraud.
- Information sharing and private-public collaboration on digital identity at a level similar to the Australian Cyber Security Centre's (ACSC) Cyber Threat Intelligence Sharing program.
- Expansion of SOCIA to classify key components of the digital identity ecosystem as CI and SONS with additional controls based on their use and their risk profile.
- A pause on further expansion of cyber security legislation until the efficacy of existing SOCIA requirements has been evaluated.

Additionally, ACT Government notes a gap in Commonwealth guidance around the inclusion of individuals/groups/organisations into the design and ongoing management of CI. With the implementation of the *SOCIA*, its likely expansion in coming years, and the heightened importance of CI and SoNS, ensuring appropriate personnel are working with/on CI is imperative. While we believe this is partially addressed by our recommended improvements to a security-cleared workforce, we also recommend the National Strategy include development of policy and guidance around CI personnel.

Inclusive design must be part of security by design

Australian governments and businesses are rapidly moving to a digital-first model, increasing the cyber security risk profile of organisations and their services. Many of these organisations consider it vital that their products are designed and deployed with multiple methods of access so the products remain usable should one or more access methods fail.

To ensure equal access to services, this approach must be a critical consideration for local, state and federal government when designing community solutions. Consultation with marginalised groups and users is also crucial, to ensure their unique requirements are addressed. Failure to do so can lead to pressure on other channels or inability to access vital services as highlighted by the myGov audit.[8]

The Digital Transformation Agency's Digital Service Standard outlines strong guidelines to embed accessibility in solution design. The National Institute of Standards and Technology's (NIST) recent Digital Identity guidelines incorporate an equity-based risk framework to map out and treat system and service level risks.[9]

Given a key focus for cyber security is to ensure we protect all Australians when using digital services, we need to ensure the National Strategy takes a nuanced approach to control implementation and ensures that secure systems are inclusive of all users.

---

[8] myGov Audit Volume 2: Detailed Analysis

[9] NIST SP 800-63-4 Digital Identity Guidelines Public Draft of Revision 4

The ACT Government recommends the National Strategy;

- mandate a collaborative and codesign approach for cyber policy, controls, and regulation when they impact the ability of a user to access a system or service
- establish inclusive-by-design requirements for organisations to incorporate into their secure-by-design approaches
- encourage the use of innovative approaches to inclusivity-by-design, such as the NIST's use of a risk-based approach to address equity, inclusion, access, security, privacy, and fraud.

Essential Eight should be the standard for all government entities

As noted previously, the Australian Government must leverage its resources and capabilities to drive cyber resilience across all levels of government. Strong steps have been taken at the Commonwealth government level with the requirement that all non-corporate Commonwealth entities must meet the ACSC's Essential Eight maturity level 2 (ML2).[10]

The National Strategy should consider an approach to drive Essential 8 maturity level 1 as the minimum standard for entities at all other levels of government. ACSC reporting regularly identifies that governments of all levels make up more than a third of reported cyber security incidents (34% combined in 2021-22).[11] Though the Commonwealth government reports approximately twice as many incidents as State, Territory, and Local governments—24% compared to 10% in 2021-22—non-Commonwealth levels of government still require comparable levels of cyber resilience. Particularly given the ongoing development of integrated approaches to digital services (notably the digital identity ecosystem), the 'blast radius' of successful attacks on non-Commonwealth governments has the potential to expand to Commonwealth level systems.

The ACSC and Australian Security Intelligence Organisation have called out the growing threat of foreign interference across all levels of government.[12,13] Given:

- the Commonwealth has set ML2 as the standard for its non-corporate entities
- organisations are meant to uplift to the maturity level appropriate to the capability of threat actors expected to target them, and
- the expected threat actors towards the Commonwealth government and non-Commonwealth governments are rapidly aligning.

It is appropriate that non-Commonwealth governments should be targeting at least ML1 uplift, however they do not have the resources necessary to do so. Barriers to uplift for ACT Government include—but aren't limited to—a significant application legacy; substantial amount of cloud hosted systems that need uplift; the need to better understand the scope of required uplift across some of our networks; a lack of skilled cyber professionals to undertake the uplift; a lack of financial resources to pay for uplift; difficulty in achieving positive security vetting of staff due to the need to hire non-citizens; and an improving but still developing cyber security culture across our organisations. These barriers will impact the speed at which ACT is able to become compliant with any standards that are set.

To this end, we recommend the National Strategy—through regulatory change—set ML1 and equivalent security control frameworks as the mandatory standard for all non-corporate non-Commonwealth government entities. Further, the National Strategy should set ML1 and equivalent security control frameworks as an expected (but not mandatory) baseline for all other government entities, including corporate.

---

[10] Policy amendment – Information security | Protective Security Policy Framework
[11] ACSC Annual Cyber Threat Report 2022
[12] ACSC Annual Cyber Threat Report 2022
[13] Director-General's Annual Threat Assessment | ASIO

Simplifying uplift

Australian governments and businesses are dependent on a marketplace of tens of thousands of software and cloud service providers to deliver digital solutions. It is challenging for organisations to know which of these are secure for their purposes. While use-cases differ between and within organisations, a searchable register of service providers and software that meet a common security criterion (i.e., the ACSC's Information Security Manual's PROTECTED security classification controls) could greatly improve the ability of organisations to find and procure appropriately secure services.

The Commonwealth Government has established similar services before, such as the Hosting Certification Framework's Certified Service Providers and the—now discontinued—Certified Cloud Services List (CCSL).[14]

We recommend the ACSC establish and manage a new register, hosted on a publicly accessible portal (most likely cyber.gov.au to leverage the ACSC's existing knowledge base and popularity). The ACSC would specify the requirements that a particular category of service must meet for inclusion on the register, such as compliance with a Relevant Document per the *SOCIA*.[15] It is important that the burden of compliance is light enough to ensure organisations of all sizes and financial capacity are able to be listed. Organisations that wish to be included in the register would obtain proof, or be supported to obtain proof of compliance for their systems/services (i.e., through an IRAP assessment of compliance with the Information Security Manual's PROTECTED security classification controls) and provide that evidence to the ACSC. Once confirmed, the ACSC would add the system/service to the register under an appropriate category.

Additionally, solutions and services on this register must be supported by configuration standards. These standards would assist procuring organisations to implement the solution/service such that it meets the level of security the product displays on the Register. This is an essential step to mitigate risks associated with mis-configured security controls and would address one of the lessons learned from previous similar registers, such as the CCSL.

This register would enable organisations with limited cyber security resources to select services/solutions known to be compliant with ACSC recommended security frameworks. The register would also make it far easier for organisations to find appropriately secure services/solutions. In turn, these improved capabilities would deliver better cyber resilience for many organisations.

A nationally consistent approach to information security classification and requirements

As noted in our June 2022 submission to the *National Data Security Action Plan* discussion paper, we are in-principle supportive of a proposal to establish consistent data security policy settings through a principles-based approach. It remains important that states and territories retain ownership of legislative and policy mechanisms which allow data and digital technologies to be used in innovative and nation-leading ways. We recommend a nationally standardised approach to data security form part of the National Strategy.

Conclusion

The cyber threat landscape has changed dramatically in the last few years and shows no signs of slowing down. ACT Government looks forward to collaborating on the National Strategy's development to make Australia one of the most cyber secure nations in the world. We recommend the creation of annual working groups that bring together private and public sectors to assess the cyber threat environment and the impact of changes in the environment on Australia's national cyber resilience.

[14] Certified Service Providers | Hosting Certification Framework; Cloud Services | Cyber.gov.au

[15] *Security of Critical Infrastructure Act 2018* (Cth) s 30ANA (2)

ACT Government direct response to discussion questions

ACT Government has provided many of our responses to the Discussion Paper's questions in the main body of our submission. This supplementary document provides additional context in a direct response to each question format.

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?

A1. Our submission and recommendations together provide a holistic response to this question.

Enhancing and harmonising regulatory frameworks

Q2. What legislative or regulatory reforms should the Government pursue to enhance cyber resilience across the digital economy?

A2. We recommend expansion of the *Security of Critical Infrastructure Act 2018* (*SOCIA*; Cth) to include digital identity services and solutions, along with policy expansion to address aspects such as the Essential Eight and a nationally standardised approach to data security.

Q3. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy?

A3. Methods that create legal obligations are the only mechanisms to improve mandatory operational cyber security standards, due to their mandatory nature. However, any method creating legal obligations must be approached with extreme caution due to the likely financial and resourcing impacts such obligations would have on entities, particularly non-Commonwealth government entities.

Q4. Is further reform to the SOCIA required? Should this extend beyond existing definitions so that customer data and systems are included?

A4. As outlined in the main body of our submission we recommend expansion of the *SOCIA* to classify key components of the digital identity ecosystem as CI and SONS with additional controls based on their use and their risk profile. We also recommend a pause on the further expansion of CI legislation (outside of the expansion we recommend above) until the efficacy of the existing *SOCIA* requirements has been evaluated.

Q5. Should the obligations of company directors specifically address cyber security risks and consequences?

A5. Obligations should exist around the protection of sensitive data. Organisations that handle such data should then inherit those obligations to their responsible entities.

Q6. Should Australia consider a Cyber Security Act, and what should this include?

A6. ACT Government is in-principle supportive of new legislation that strengthens Australia's cyber resilience. However, without any detail on the contents of the legislation or the obligations it will impose, we cannot comment further. Given such detail does not exist about a Cyber Security Act, we suggest that it would be better to consider what legislative reforms are both needed and not more appropriately located in other legislation before considering a new Act.

We also recommend pausing any further expansion of *SOCIA* legislation and other cyber security legislation until such time as the efficacy of the existing *SOCIA* legislation has been evaluated.

Q7. 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?

A7. Nil Response

Q8. 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?
A8. We consider this a sensitive topic and will provide our input through other channels.

Q9. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies, and insurers?
A9. We consider this a sensitive topic and will provide our input through other channels.

Q10. 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?
A10. We consider this a sensitive topic and will provide our input through other channels.

Strengthening Australia's international strategy on cyber security

Q11. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?
A11. Nil Response

Q12. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?
A12. Nil Response

Q13. 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?
A13. Nil Response

Securing government systems

Q14. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?
A14. We strongly support the ACSC's ongoing work in delivering cyber security information, policy, and guidance to the Australian community and would encourage expansion of this advice where appropriate and in line with the forthcoming National Strategy. The Commonwealth Government can further serve as a model for other entities by resourcing uplift to Essential Eight Maturity Level 2 for its non-corporate entities, per the Commonwealth's Protective Security Policy Framework. This resourcing commitment would strengthen business cases for other organisations seeking Essential Eight uplift.

Improving public-private mechanisms for cyber threat sharing and blocking

Q15. What can government do to improve information sharing with industry on cyber threats
A15. We support the Commonwealth's CITAS program, in their role as the responsible entity for providing national threat intelligence. We also recommend a similar model of information sharing should exist for threats to the digital identity ecosystem.

Q16. During a cyber incident, would an explicit obligation of confidentiality upon the ASD ACSC improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ACSC without the concern that this will be shared with regulators?
A16. Nil Response

Q17. Would expanding the existing regime for notification of cyber security incidents improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?
A17. Nil Response

Q18. What best practice models are available for automated threat blocking at scale?
A8. Nil Response

Supporting Australia's cyber security workforce and skills pipeline

Q19. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?
A19. Yes. Please see our main submission for detail.

Q20. What more can the Australian Government do to support Australia's cyber security workforce through education, immigration, and accreditation?
A20. Please see our main submission for detail.

National frameworks to respond to major cyber incidents

Q21. How should the Government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?
A21. We recommend the Commonwealth Government have an on-call capability who can respond in the event of major cyber incidents (as they are defined under legislation). The Commonwealth should also take a leading role in ensuring Australians know where to go to obtain information about how an incident impacts them.

Q22. Should Government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?
A22. Yes.

Q23. What would an effective post-incident review and consequence management model with industry involve?
A23. Nil Response

Community awareness and victim support

Q24. How can Government and industry work to improve cyber security best practice knowledge and behaviours and support victims of cybercrime?
A24. Nil Response

Q25. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?
A25. Nil Response

Investing in the cyber security ecosystem

Q26. 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?
A26. A variety of opportunities exist for Government to achieve this, such as subsidies to organisations, GST exemptions, and our recommendation for a register of security framework compliant services and solutions.

Q27. How should we approach cyber security technologies future-proofing out to 2030?
A27. Nil Response

Q28. Are there opportunities for Government to better use procurement as a lever to support the Australian cyber security technologies ecosystem and ensure there's a viable path to market for Australian cyber security firms?
A28. While not a comprehensive solution to this problem, we believe the register of security framework compliant services and solutions recommended in the main body of our submission would assist with this challenge.

Designing and sustaining security in new technologies

Q29. How should the Strategy evolve to address the cyber security of emerging technologies and promote security-by-design in new technologies?
A29. Nil Response

Implementation governance and ongoing evaluation

Q30. How should Government measure its impact in uplifting national cyber resilience?
A30. This is a significant challenge as many forms of measurement in this space could make the situation seem worse, when it's just improved data (i.e., rapidly increasing amounts of reported cyber attacks could be both an increase in attacks and an increase in reports that previously would have been unreported). One method that may help measure impact is tracking compliance with Essential Eight maturity levels (or equivalent framework) through mandatory reporting for Critical Infrastructure, and opt-in reporting for other organisations.

Q31. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?
A31. Nil Response