Department of Home Affairs
Submitted electronically via Department of Home Affairs Submission Form

21 April 2023

2023-2030 Australian Cyber Security Strategy Discussion Paper

AGL Energy Limited (**AGL**) welcomes the opportunity to provide an input on the questions raised in the 2023-2030 Australian Cyber Security Strategy Discussion Paper released by the Expert Advisory Board of the Department of Home Affairs (**Department**).

AGL is a leading essential services provider with a 185-year history in the provision of gas and electricity, and since 2020, telecommunications services to customers throughout Australia. AGL has been heavily involved in the development of the Australian Energy Sector Cyber Security Framework (**AESCSF**), to ensure that the energy sector's security posture is uplifted and prepared for the increasingly complex cyber threat landscape.

In addition, AGL has been involved in the co-design process for the Security of Critical Infrastructure reforms including the amendment of the *Security of Critical Infrastructure Act* 2018 (Cth) (**SOCI Act**) and the associated rules.

AGL, like many organisations, considers several key principles and themes when developing its cyber security strategy. Key themes relevant to the 2023-2030 Australian Cyber Security Strategy include:

- Trust: A critical outcome of the strategy is the creation of a safe, trusted, and secure digital environment. Improving trust and confidence in Australia's cyber security resilience to an evolving cyber threat landscape by maturing cyber security capabilities across government and industry is fundamental to achieving this outcome.
- Culture: Cyber security excellence needs to be grounded in embedded awareness and culture at all levels. Everyone has a role in making Australia a world leader in cyber security and resilience.
- Leadership: Emphasise the importance of good leadership in cyber security, the role of leaders in fostering a cyber aware culture, driving action to protect systems and data, and report incidents.
- Collaboration: Cyber security resilience requires broad collaboration and alignment, between Australia and other countries, between government and industry, and between industry entities.
- Simplification: Simplify, strengthen and align cyber security legislation, regulation and policy. Simplify compliance processes and reporting of cyber security incidents or privacy breaches.
- Talent: Australia is facing a massive cyber security talent shortage, and it must attract, retain, and invest in cyber security talent development and build a future-fit workforce.

Please find in Attachment 1 AGL's responses to the questions asked in the discussion paper. Our submission does not contain any confidential AGL information.

AGL looks forward to working with the Department to ensure that the 2023-2030 Australian Cyber Security Strategy is fit for purpose and considers energy specific issues.

If you have any further questions about this submission please contact Stuart Hay, Senior Manager Cyber Regulatory and Compliance Liaison at shay2@agl.com.au.

Yours sincerely,
Maryam Bechtel
AGL Chief Information Security Officer

Attachment 1: 2023-2030 Australian Cyber Security Strategy Discussion Paper – AGL responses

Question 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?

In our view, to make Australia the most cyber-secure nation in the world by 2030, the strategy should incorporate consideration of the following key ideas:

1. Clear and holistic vision: articulate a coherent vision for cyber security in Australia, encompassing all levels of the economy and community. Such a vision would focus on key themes of leadership, trust, simplification, collaboration, and alignment. It would set clear, measurable objectives and outcomes for cyber security and provide a roadmap for achieving them.
2. Leadership and culture: emphasise the importance of leadership in fostering a positive security culture across Australia. Bring government, business, and industry leaders together to drive a shared and aligned approach to cyber security risk management and mitigation to better achieve established objectives and outcomes.
3. Collaboration and alignment: Government and regulatory authorities should engender a willingness to work together with each other and with organisations to collectively understand and address shared problems and scenarios, as well as to identify and harness best practice. Consideration should also be given to facilitating collaborative cyber security efforts to achieve shared objectives and outcomes.
4. Trust and resilience: prioritise building trust across all levels, including trust in data, products, services, and entities. Address resilience as a core trust enabler, particularly preparedness for and response to cyber threats and incidents, in the face of dynamic global contexts, particularly with extensive and at times vulnerable global supply chains.
5. Standardisation and accessibility: establish mechanisms and incentives to drive consistency and alignment of cyber security measures across all levels, including clarity on what effective cyber security baseline capabilities look like. Make cyber security baselines accessible and affordable for all, including consumers, and small and medium businesses. Doing so will help address significant challenges faced by the least resourced entities and help strengthen supply chains. Enable clear communication and shared understanding by defining terminology and driving shared meaning, including key cyber, security, risk and resilience concepts and terms.
6. Simplification and consistency: remove overlapping layers of legislation and regulation relating to cyber security and privacy, and harmonise the compliance processes and reporting of cyber security incidents or privacy breaches to government bodies and regulatory authorities.

By incorporating these key ideas into the strategy, Australia can work towards becoming the most cyber-secure nation in the world by 2030. With effective leadership, collaboration, and alignment, along with consistent and accessible cyber security measures, Australia can create a secure and resilient cyber landscape that protects its economy, community, and critical infrastructure from evolving cyber threats.

Enhancing and harmonising regulatory frameworks

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

A key reform with the potential to significantly contribute to enhancing cyber security in Australia is the simplification of the legislative and regulatory frameworks. Doing so would help minimise the regulatory burden on organisations, making it easier to understand, implement, and maintain effective cyber capabilities.

To achieve regulatory simplification, the government would need to take steps to simplify, streamline, and harmonise existing legislation, regulations, and regulatory guidance across Australia, including Commonwealth, State, and Territory governments.

Providing clear and well-defined legislated/regulated security requirements will help to ensure a minimum level of security maturity or control posture across Australia, promoting a consistent and effective approach to cyber security across all sectors. It would also enable better alignment of cyber security practices across sectors and supply chains, facilitate greater collaboration and information sharing among stakeholders and ultimately strengthening the overall cyber security posture of the nation.

By taking these measures, Australia can create an environment that fosters cyber security excellence, reduces compliance burdens on organisations, and promotes a collaborative and aligned approach to addressing cyber threats. Doing so will contribute to building a more secure and resilient cyber landscape across Australia, protecting critical infrastructure, sensitive data, the interests of the public and private sectors, and the digital economy.

Question 2.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)?

AGL, like many Australian organisations, is subject to multiple legislative and regulatory obligations, many of which incorporate mandatory operational cyber security standards or requirements and cyber security incident or privacy breach reporting obligations. As indicated in our response to Question 2 above, simplification would deliver several significant benefits.

Simplification of this environment will require a multi-faceted approach across various regulatory frameworks. Australian governments and regulatory authorities could collaborate to identify, harmonise, streamline, and simplify the various legislative and regulatory standards and requirements for cyber security. A very challenging endeavour.

One potential solution is the creation of a Cyber Security Act (CSA) providing a comprehensive legislative framework that sets out minimum operational cyber security standards and requirements for all organisations, regardless of sector or industry. This would simplify the regulatory landscape, reduce compliance burdens, and harmonise the consistency of cyber security across Australia.

Alignment of cyber security standards and requirements across all Australian jurisdictions may be simplified by reference to CSA in relevant laws and regulations, giving organisations a single set of cyber security standards and requirements to adhere to, reducing confusion and promoting compliance. This simplification will help organisations to prioritise cyber security as a strategic imperative and drive the integration of cyber security into all aspects of their operations.

Like many other sectors, the energy sector faces some unique cyber security threats and challenges due to the nature of its operations, data handling requirements, and the potential impact of disruptions. Tailored regulations for specific sectors, with reference to CSA, can provide more explicit and practical standards and requirements for specific environments or situations, enabling more effective cyber security controls and measures to be implemented. Such regulations and guidelines can take into consideration sector-specific treats, risks, and secure practices to provide clear guidance to enable compliance with CSA.

Consideration should also be given to clarifying standards, requirements and liabilities associated with the security of products and services. Doing so may incentivise organisations to prioritise cyber security in product and service management and delivery, resulting in safer and more cyber secure products and services being made available.

Question 2.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?

The *Security of Critical Infrastructure Act* 2018 (Cth) (**SOCI Act**) should not be extended to explicitly include customer data and systems within the definition of 'critical assets'. In many cases, customer data or systems are not required to support the effective operation of critical assets or the delivery of essential services, this is the case for energy generation. That said, data is often a critical dependency for the secure and effective operation of critical infrastructure products and services, this is the case for energy generation. Critical data, along with the associated storage and processing capabilities, should be identified and protected accordingly. While the SOCI Act already incorporates data-related requirements, these requirements could be made more explicit, as outlined above.

Existing Privacy legislation and Consumer Data Rights (CDR) regulations address the privacy aspects and protection of personal information and consumer data records. Where there is an overlap in reporting obligations, for example, if a cyber security incident requires reporting to the ACSC under the SOCI Act and reporting to the OAIC under the *Privacy Act 1988* (Cth) (**Privacy Act**), it would be simpler to have one set of reporting obligations rather than having to report separately to two different bodies or regulators.

As indicated in our response to questions 2 and 2.a, regulatory reform would simplify and clarify cyber security standards and requirements, aligned across key laws and regulations, including the SOCI Act, Privacy Act and CDR, enabling a more cohesive and comprehensive framework for addressing the protection of confidential and commercially sensitive Australian data and systems, including personal information and sensitive information of individuals.

Question 2.c: Should the obligations of company directors specifically address cyber security risks and consequences?

For companies such as AGL that identify cyber security and resilience as a strategic business risk, directors already have an involvement in monitoring and managing the risk without the need to overlay any additional, specific duties. We note, the SOCI Act already requires board approval of annual reports in relation to their critical infrastructure risk management program.

Existing directors' duties already require directors to take all reasonable care and steps to ensure that the material business risks are appropriately understood and mitigated against. While the

nature of the risks and the steps required to manage and mitigate them will be different depending on the risk area, the overarching duties framework for directors is already well understood and consistently applied across the different risk areas (whether it be cyber security or climate change).

Overlaying additional, specific duties will only serve to complicate rather than clarify the obligations of directors, and we do not see any compelling reason as to why cyber security should be singled out for a differentiated approach.

Question 2.d: Should Australia consider a Cyber Security Act, and what should this include?

Australia should consider a Cyber Security Act (CSA) as a key element of a broader regulatory reform program. More regulation without a simplified, clearer, streamlined, and harmonised regulatory environment is not desirable. Our responses to questions 2 and 2.a provide more detail.

A CSA should specify a minimum-security baseline, rather than specify best practice ideals. It should provide clarity on the cyber security objectives and outcomes to be achieved and allow flexibility in the application of mechanisms contextually based on criticality, classification, or risk.

The SOCI Act, like many other security frameworks, incorporates an all-hazards-based approach, including personnel, physical/natural, supply chain and cyber threats or hazards. A CSA should clearly indicate its scope, boundaries, and application in this context.

Question2.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?

Our responses to questions 2, 2.a and 2.b outline the opportunities for regulatory reform to create a simplified, clearer, streamlined, and harmonised regulatory environment.

Like measuring costs and value from cyber security investments and operations, measuring the burden associated with regulation and regulatory reforms is exceedingly challenging, particularly in complex, dynamic and highly integrated technology and cyber threat environments.

Lacking fully defined rules, previous regulatory impact estimations for SOCI were of limited value to AGL and probably to government, resulting in broad estimates and significant assumptions that may not accurately reflect the true costs associated with reforms.

Increased collaboration between the government and industry to progressively elaborate and refine impact estimates will assist all parties to better understand the key drivers of impact. Regular reviews of estimates and actual costs will help to improve their accuracy and relevance. This iterative approach may also help to identify opportunities to further streamline regulatory frameworks, reduce unnecessary burdens, and ensure that regulatory measures are effective in enhancing cyber security without unduly hampering business.

Question 2.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?

AGL agrees with the premise that criminals should not profit from their crimes. Prohibiting the payment of ransom or extortion demands may reduce the volume of attacks. However, such a prohibition may result in potentially avoidable catastrophic damage, harm to community, loss of life, disruption of essential services or disclosure of sensitive information. In some circumstances and for some organisations, the payment of a ransom demand may be the only path to achieving acceptable outcomes.

Instead, government should strongly discourage payments and revisit imposing such a prohibition when Australia has more resilient cyber security capabilities in place. Mandatory reporting of every instance where a ransom demand is made, may enable better understanding of the nature and scale of the problem. It would also enable situational approaches to be applied, providing flexibility in ransom payments based on the severity of potential impacts to the victim and consequential harms to others.

Question 2.f.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?

A strict prohibition of the payment of ransom or extortion demands may have unacceptable consequences for victims, insurers, customers, and communities. Our response to 2.f provides further details.

Question 2.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 clarification on its position with respect to ransom demands would be helpful. As indicated in our response to question 2.f, we think government should strongly discourage the payment of ransoms, acknowledge there may be situations where payments provide the only acceptable path, and indicate intent to revisit prohibition when Australia is in a more cyber resilient state.

Government can take a more active leadership role to help victim organisations and individuals to make better informed decisions on whether to pay a ransom, with consideration given to all relevant matters, including consequential harms across stakeholder groups.

Strengthening Australia's international strategy on cyber security

Question 3: How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

While AGL's asset portfolio is located in Australia and it interacts with Australian customers and communities, our supply chain providers are located globally with products and services sourced from many countries. Opportunities to work with our neighbours should be explored, including opportunities for collaboration to improve regional and global threat intelligence sharing, mutual support and collaborative responses to cyber incidents, sharing of lessons learned, fostering cyber

talent development, and engaging in joint research and development efforts to enhance security products and capabilities.

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

The simplification and harmonisation of cyber security standards and minimum baselines with Australia's international partners, would help the alignment and consistency of cyber security requirements and capabilities through our extended global supply chains, leading to improved cyber resilience. It would also reduce the regulatory burden for organisations operating across multiple jurisdictions.

Accreditations and certifications recognised across international jurisdictions, providing assurance that products and services meet cyber security standards, would help engender trust in those products and services for use in critical infrastructure, supply chains, and sensitive environments.

Question 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?

As indicated in our response to question 4, Australia can lead through the simplification and harmonisation of its cyber security standards and minimum baselines.

Securing government systems

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

Government entities, at all levels, should be leaders and models for better practice cyber security capabilities, particularly those entities that handle sensitive information and provide critical services. This includes achieving the requirements specified in relevant frameworks such as the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM).

It is very concerning that a significant number of government entities fail to achieve Essential Eight maturity, and significant exposures and capability gaps continue to be identified in government audits and reviews at all levels of government. Government must show leadership by accelerating the hardening of government systems in line with relevant requirements.

Trust in government, including trust in digital and online services, data protection, and resilient service delivery, should be prioritised at all levels. The government should demonstrate what good cyber security looks like, acknowledge areas where good enough is not being achieved, and take proactive action to mitigate and remediate identified shortcomings.

Improving public-private mechanisms for cyber threat sharing and blocking

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

Government can improve information sharing with industry on cyber threats by:

1. declassify and broadly share relevant threat intelligence to provide timely and comprehensive information to industry stakeholders.
2. streamline information and processes to make it easier for companies to receive and use threat intelligence information. This may be achieved through the development of standardised reporting formats or the use of automated tools for sharing information.
3. coordinate, facilitate and support information-sharing networks within the industry by providing guidance, resources, and coordination efforts. This could involve establishing common practises, protocols, and platforms for information sharing, particularly for operational and tactical intelligence, to enhance the overall understanding of the threat landscape within the industry. Intelligence sharing must be done in an organised and systematic manner using standard sharing protocols due to the volume and lifespan of such information, to enable operational efficiency for sharers and recipients, and ultimately to enable prioritised and effective action to be taken.
4. consolidated intelligence to provide higher level understanding of the threat landscape for Australian industry sectors. Consider enabling or requiring threat intelligence feeds from critical infrastructure entities to achieve this.

By fostering collaboration and information sharing, government can contribute to a more resilient and secure cyber ecosystem, leading to improved cyber threat awareness and response capabilities.

Question 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?

Collaboration and trust among all entities involved in a cyber incident response is critical for achieving timely and effective outcomes. Safe-harbour protections would enable sharing relevant sensitive/personal information during cyber incidents to better respond to and mitigate against potential harms.

To facilitate this, mechanisms for operational security need to be established to ensure that information shared during an incident remains secure and does not get intercepted by threat actors or otherwise fall into the wrong hands.

Question 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?

Expanding the existing regime for notification of cyber security incidents, to require mandatory reporting of ransom or extortion demands, may help to improve understanding of the nature and scale of these cybercrimes.

Analysis of reports and reporting data may be leveraged to build awareness through alerts and advisories, broader awareness campaigns, case studies, self-assessment tools, and exercise scenarios, delivered via a range of communication channels, including news and social media. The use of actual examples and showcasing the nature, scale and impacts of ransomware and extortion,

can help people to gain a better understanding of the seriousness of these cyber threats and the need for robust cyber security measures. It would also help counter some of the misconceptions and misinformation provided by some channels.

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

Best practice models for automated threat blocking at scale typically involve the use of threat intelligence feeds that provide real-time updates on emerging threats contextualised to the environment being protected. These feeds are used to automatically block suspicious traffic or activities based on predefined rules or patterns, leveraging artificial intelligence (AI) and machine learning (ML) capabilities.

Automated threat blocking is not without its challenges. The potential for false positives, where legitimate traffic or activities are mistakenly blocked, may result in significant disruption of services. Different vendors may use varying risk and confidence scores on intelligence artefacts to push for automated blocking, and threat actors may bypass automated blocking by disguising their tactics, techniques, and procedures (TTPs) to simulate legitimate traffic or activity. The use of AI and ML technologies can help improve the accuracy and effectiveness of automated threat blocking, along with the secure processing of legitimate activity, at scale. Broader adoption of zero trust capabilities will also help, by automatically blocking all untrusted traffic and activity.

Supporting Australia's cyber security workforce and skills pipeline

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

The government's broader STEM (Science, Technology, Engineering, and Mathematics) agenda helps to deliver key foundational knowledge and skills required by cyber security professionals. However, a broader tailored approach is required to uplift cyber skills in Australia.

Cyber security encompasses a broad range of areas, while it should focus on cyber-specific capabilities, all-hazards need to be addressed, including personnel, supply chain and physical/natural hazards. Clear pathways and frameworks for learning, development, and certification should be established, and aligned with future cyber job opportunities.

An education and awareness campaign led by government could highlight and promote rewarding careers in cyber security to a broader audience. It could emphasise how getting and staying ahead of hackers and protecting sensitive data, systems and services can be an exciting career prospect for the generations growing up in a world full of high-profile breaches.

Not all cyber security roles require STEM backgrounds, there is a need for clear cross-skilling pathways for individuals who may not have a STEM background but possess other relevant and desirable skills and knowledge. People with diverse non-cyber backgrounds should also be encouraged and supported in transitioning into the cyber workforce through appropriate training and development programs, such as the Cyber Academy program, which fosters new cyber talent. Government support of these programs would enable expansion across more universities and organisations, helping to uplift cyber skills by tapping into broader talent pools.

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

The shortage of skilled cyber professionals, which is exacerbated by factors such as digital transformation, regulatory changes, government and industry initiatives, cyber incidents, and competing demands in areas such as data science, automation, and AI. Government can do more to support Australia's cyber security workforce through education, immigration, and accreditation. Government should consider a range of measures to help attract, develop, and retain cyber security talent.

Increase funding to universities and TAFE to create more places for relevant courses, and to ensure entry requirements are not unreasonably high due to limited course spaces. This may include funding to train females and other under-represented cohorts to increase the diversity (gender, cultural and socio-economic), and subsidies for employers willing to hire them in roles that lead to careers in cyber security.

More can be done to encourage the cohort of primary and secondary school digital natives to consider a career in cyber security. Promoting cyber-related learning outcomes and awareness of the roles and opportunities in cyber security, may attract students who would otherwise consider more visible or well-known professions or trades.

Streamline and fast-track visa and sponsorship applications for internationally qualified talent to attract suitable cyber talent from overseas. This may include allowing international students studying cyber security to work more than the current limitation of 48 hours per fortnight and making it easier for Temporary Graduate visa (485) holders to enter the industry. Creating a straightforward pathway to transition from 485 to permanent residency may also help retain international talent.

In the dynamic and fast-paced cyber security environment, continuous development of technical skills and knowledge is critical for effective and secure operations. Establishing a nationally recognised cyber security professional scheme or certification based on relevant standards can ensure that those working in the field are properly qualified, skilled, experienced, and ethical.

Government support for certification programs, micro-credentialing, and incentives to encourage employers to invest in developing, retraining, and upskilling of cyber security talent. This may include clear subsidised pathways into cyber-related education and vocational programs offering real-life experience in the industry, free or discounted courses for cross-skilling, and tax breaks for cyber security professionals. Broad cyber awareness and cross-skilling is likely to deliver significant value with most jobs involving the handling information and technology, enhanced cyber knowledge and skills will help to better protect it.

National frameworks to respond to major cyber incidents

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

Australia is highly interconnected, with critical dependencies across multiple sectors particularly the energy sector which is critical for effective continued operation of other sectors. Beyond existing law enforcement and operational responses, careful and coordinated management of interdependencies during responses to major cyber incidents is necessary to effectively protect Australians.

To be effective, collaboration among relevant stakeholders and organisations is required to deepen the shared understanding of the threats and risks, as well as critical capabilities in place to protect the infrastructure and services Australia relies on. This collaboration should extend throughout the entire incident management lifecycle, from identification and preparation to protection, detection, response, and recovery. Developed capabilities need to be periodically tested, reviewed, and adjusted to continuously improve and adapt to the changing environment, and to ensure they remain appropriate and effective.

Government should lead and enhance Australia's cyber resilience, particularly its preparedness for cyber incidents. This may include developing aligned plans, playbooks, detection methods, training, and exercises, and practising them together with relevant entities. Post-incident reviews and lessons learned should be completed for all significant Australian cyber incidents, as well as learning from international incidents, to improve Australian preparedness and response capabilities. Case studies from past cyber incidents can be leveraged to identify good practises and areas for improvement.

Government should also lead the building of cyber-awareness throughout the community. Early detection of cyber threats enables quicker response and mitigation. Efforts should be made to help people spot and deal with scams, social engineering attacks, and suspicious behaviours. This can be achieved by strengthening cyber security awareness and providing clear guidance on what to do and who to contact for help in the event of a cyber incident, through multiple channels.

A cyber-aware culture, individuals, and organisations, is better equipped to prevent, detect, and respond to cyber threats, ultimately enhancing Australia's overall cyber security posture and resilience.

Question 13.a: Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

Like many Australian entities, AGL is required to report cyber incidents to multiple bodies or regulators, in varying levels of detail, format and timeframes. Implementing a single reporting portal for all cyber incidents would greatly simplify the reporting process and improve efficiency.

A single reporting platform would ensure reports are standardised and contain the necessary level of detail, making it easier for relevant government bodies and regulators to understand and respond appropriately to the incidents. Doing so would help save time and valuable resources better utilised in responding to the incidents and mitigating their impacts, and would contribute to a more coordinated and efficient response to major cyber incidents, enabling the coordination indicated in our response to question 13.

In addition, government should consider strengthening cyber incident reporting obligations to require organisations experiencing a cyber incident to promptly notify all impacted parties, including customers, suppliers, and partners. In the absence of such an obligation, organisations often rely on their contractual counterparts to notify them (whether or not adequate contractual protections are incorporated in relevant agreements or arrangements). This requirement is missing in the SOCI Act, which should align with the notifiable data breach regime under the Privacy Act (where organisations have an obligation to notify affected individuals).

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

An effective post-incident review and consequence management model with industry would prioritise collaboration and information sharing to identify best practises and stay updated on emerging and heightened threats.

As leaders, Government would bring together relevant industry stakeholders in a structured review process to analyse incidents and the consequential impacts of them, identify areas for improvement, and propose changes to enhance cyber security resilience and defences. Underpinning the success of this approach is the open sharing of relevant information, our responses to questions 7 and 8 provide further details.

Government led collaboration would foster a proactive and adaptive approach to cyber security, leveraging expertise and insights from all participants, facilitate improvement in cyber security preparedness and response, and leading to more robust and resilient cyber security practises across Australia.

Community awareness and victim support

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

The value of identity data and artefacts is significant in Australia. For organisations, such as AGL, with the need to collect personal information to verify the identity of customers, employees, suppliers, and others and to conduct credit checks and assessments, significant cost is expended to handle and protect identity data and artefacts. For individuals, the exposure of identity data and artefacts creates potentially significant harms, such as identity theft.

Government could establish a single, centralised government identifier for all individuals across Australia, and set up a digital identity platform that enables organisations to verify the identity of individuals without requiring them to provide personal information, government identifiers or copies of identity artefacts. This can significantly reduce the value of gaining access to such information and reduce the potential harm to individuals whose personal information, government identifiers or identity artefacts has been leaked or exposed. It would also make it more difficult for criminals to profit from their attacks, deterring them from targeting Australian organisations and individuals.

To balance cyber security with privacy concerns and protect Australians from potential abuse of digital identity information and platforms, government should secure them so they can only be used in specific contexts, and not susceptible to potential misuse by government or data aggregators.

Question 15.a: What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

AGL, like many other Australian organisations, engages a significant number of small businesses in our extended supply chain, including businesses delivering products and services critical to the effective continuous delivery of AGL products and services. The actions and capabilities outlined in our responses to other questions should be scalable and accessible for all organisations, including small businesses.

Small businesses have limited resources and capabilities to deal with complex cyber security requirements and incidents, which can make them more susceptible to taking risks that could compromise their security. Government should consider opportunities to assist small businesses to review and uplift their cyber security capabilities. By providing clear and concise guidance that is scalable or tailored to the needs of small businesses, the government can help promote a culture of cyber security awareness and preparedness, and drive security improvements.

Investing in the cyber security ecosystem

Question 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?

Our response to question 18 outlines opportunities to enhance trust in suppliers, products, and services through accreditation mechanisms.

Our response to question 19 outlines opportunities to enhance secure-by-design and through life practices. This may involve incorporating built-in anomaly detection and automated correction mechanisms, and leveraging artificial intelligence (AI) where appropriate, to proactively detect and mitigate cyber security threats. By prioritising security and privacy in the design and development of technologies, government can foster a culture of cyber security resilience and encourage the uptake of secure technologies across Australia's cyber security ecosystem.

Our response to question 12 outlines opportunities to enhance trust in individuals through certification and micro-credentialing. Government should consider opportunities to establish a reliable system for verifying the certifications and credentials of individuals working in cyber security, perhaps in combination with a digital identity platform outlined in our response to question 15.

Our response to question 17 outlines opportunities for government to promote cyber security research and development. Government should consider incentives to support and encourage organisations that proactively invest in enhancing cyber security capabilities, particularly capabilities sourced from Australian suppliers.

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

Government can leverage the expertise of Australian research organisations, grants, and tax incentives to encourage investment in research and development of more cyber secure products and services, with a focus on emerging technologies as well as hardening existing products and services against emerging cyber threats. This will help Australia stay at the forefront of cyber security innovation and ensure that our technologies are robust against evolving threats.

Government can also take action to attract top talent from overseas to contribute to the development of our cyber security technologies. This can be done through talent acquisition programmes, international partnerships, and a supportive environment for skilled professionals to work in and contribute to the Australian cyber security ecosystem.

Question 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?

Government can leverage its procurement to support and foster the growth of the Australian cyber security ecosystem, by requiring accredited supply of products and services to all government entities, in line with simplified cyber security standards and requirements. Broad implementation of supplier, product, and service accreditation mechanisms will enhance trust in and reliability of partners, suppliers, and service providers. Through broad accreditation, government can promote a clear path to market for Australian cyber security firms and create a level playing field for them to compete.

Government should share information regarding trusted and accredited partners, suppliers, service providers, products, and services. Doing so can foster collaboration and information sharing, enabling cyber threats in supply chains to be addressed more effectively.

Designing and sustaining security in new technologies

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

Government can prioritise secure-by-design and through-life requirements in all products and services it sources through accreditation mechanisms. Doing so will ensure cyber security considerations are integrated into the entire lifecycle of procured products and services. Our response to question 18 provides further details.

Our response to question 17 outlines actions government may take to address cyber security of emerging technologies.

Implementation governance and ongoing evaluation

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

The ultimate, albeit lagging, measure of the impact of cyber resilience uplifts is reduction in the volume, severity, and consequences of cyber incidents. Leading measures may include changes in cyber security maturity and posture, as well as the outcomes of assessments and exercises.

Acknowledging the significant variation in cyber security capability maturity across Australia, as indicated in our responses to question 2, government should simplify security standards and requirements, and establish minimum baseline standards. Doing so will help organisations understand what is expected in terms of cyber security capabilities and enable measurement of security maturity and posture.

Applying situational context will enable organisations to adopt cyber security measures that are proportionate and realistic to the cyber threats, risks, and challenges they face, as well as the criticality of the products and services they deliver. Doing so will enable alignment and benchmarking of cyber security maturity and posture across sectors and Australia. It may also foster a culture of continuous improvement, as organisations strive for better cyber security practises beyond the minimum baselines.

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

Through the implementation of an open and transparent evaluation framework, along with periodic strategic prioritisation and adaptation of the Strategy, roadmap and key initiatives, the government can demonstrate accountability, deliver ongoing transparency, and obtain valuable input into the implementation of the strategy. Doing so will provide a clear and transparent view of the government's efforts in enhancing cyber security, enable adjustments to be made in line with input and feedback from stakeholders, as well as in response to changes in the environment, fostering a more agile and responsive approach to cyber security. Periodic adaptation of the strategy will ensure it remains relevant and effective in addressing evolving cyber threats and challenges, and enable government to proactively adjust its approach, resource allocations, and align with the changing cyber security landscape.