6 February 2023

Department of Communities, Housing and Digital Economy
GPO Box 806
BRISBANE QLD 4001

Email: CyberSecureQld@qld.gov.au

Dear Sir/Madam,

RE: CYBER SECURE QUEENSLAND STRATEGIC PLAN

We welcome the opportunity to provide our views on the Cyber Secure Queensland Strategic Plan (**Cyber Plan**) prepared by the Department of Communities, Housing and Digital Economy.

We are strongly supportive of a cyber security strategic plan being introduced in Queensland that:

- consolidates existing State and Federal initiatives and resources;
- incorporates and aligns with nationally accepted best practice; and
- introduces specific objectives and targets to achieve cyber awareness and cyber resilience in Queensland across the community, business and Government.

We suggest a specific focus in the Cyber Plan on real estate dealings and transactions, given the prominence of cyberattacks targeting real estate professionals and other property stakeholders in Queensland.

Real estate businesses are a lucrative target given their involvement in facilitating high-value transactions and with the volume of personal information and data they are required to hold to properly carry out their duties.

For these reasons, we believe there is a substantive opportunity to address cyber security within real estate business in Queensland by developing a robust and effective Cyber Plan.

We would be pleased to discuss any of the matters raised further and invite you to contact Ms Katrina Beavon, General Counsel and Company Secretary of the REIQ at kbeavon@reiq.com.au.

Yours Sincerely

Antonia Mercorella
Chief Executive Officer

CYBER SECURE QUEENSLAND STRATEGIC PLAN

Submission to
Department of Communities, Housing and Digital Economy

The Real Estate Institute of Queensland (REIQ)

The REIQ is the peak body representing real estate professionals across Queensland. As the State's most trusted and influential advocate for real estate business interests and private property investor rights for more than 104 years, the REIQ remains committed to ensuring the highest levels of professionalism and good governance are achieved through regulatory compliance and the advancement of best practice standards of professional conduct.

The REIQ's enduring purpose is to lead a sustainable industry which continues to make significant contributions to the Queensland economy and to strengthen conditions for those working within the industry. Above all, the peak body aims to:

- Make important contributions to government legislation and policy settings;
- Advocate for balanced regulations for the benefit of all stakeholders;
- Provide industry-leading training for real estate professionals;
- Deliver timely, innovative and market-driven education programs;
- Promote risk management and increase professional competence;
- Implement effective and compliant professional standards; and,
- Contribute to substantial industry research and development.

Membership and customer representation includes over 30,000 property professionals. This includes principal licensees, salespeople, property managers, auctioneers, business brokers, buyers' agents, residential complex managers, and commercial and industrial agents in Queensland.

Collectively, Queensland's real estate sector directly employs over 46,000 people (the State's second largest employer), is one of the top four industries which comprises over 50% of Queensland's small business landscape, and pays the second highest amount of State tax each year (2018/19: $20 billion).

WE HELP MORE THAN OUR MEMBERS

The REIQ's vision statement, for the real estate profession, extends our support and expertise beyond our membership to the broader real estate profession and community. We believe everyone should be able to make educated, informed decisions about buying, selling or renting property and business in Queensland.

1. OBJECTIVE OF THE CYBER PLAN

Queensland is one of the few States in Australia without a dedicated cyber security strategic plan.

In the current climate, we consider the development of an effective plan is not only essential to progress our society but is a measure of good governance of our State.

As outlined in the Consultation Paper, cybercrime has become a risk of using technology in everyday life across all sectors of our community including Government, business and individuals.

On review of the Cyber Plan, there is an obvious omission of consideration given to nationally accepted best practice and a deficiency of information as to how the State intends to formulate objectives and deliverables of the Cyber Plan. We look forward to progress in this regard.

Nonetheless, we do support the overarching objectives of this proposal to:

- give Queensland the opportunity to build infrastructure and services that are cybersecure;
- strengthen partnerships across all tiers of government, industry, academia to address the greatest challenges and sharing threat intelligence so we are all better prepared;
- prepare a cyber workforce of the future; and
- attract new roles, businesses and investments into Queensland promoting as a safe and secure place.

We note this proposal does align with a core objective of the Department of Communities, Housing and Digital Economy (the **Department**) Strategic Plan 2020-2024[1], to improve technology and digital assurance by guiding government investments decisions, developing and implementing strategies and policies, addressing cyber security and driving digital capability programs.

Although it is noted that the Department has begun conversations across State Government agencies, statutory bodies, government owned corporations and local government to identify existing challenges and opportunities for improvement, we hold concern that the development of an effective plan and deliverables may not be attainable within a reasonable time.

In this regard, we suggest the development of this plan is given a high priority with a strong focus on what key deliverables to be achieved in the Cyber Plan.

[1] Department of Communities, Housing and Digital Economy (the Department) Strategic Plan 2020-2024: https://www.chde.qld.gov.au/__data/assets/pdf_file/0015/12174/strategicplan2020-24.pdf

2. EXISTING STATE AND FEDERAL FRAMEWORK

The Cyber Plan is stated to compliment other State and Federal initiatives including:

- Queensland Government Cyber Security Unit;
- Department of Employment, Small Business and Training funding initiatives;
- Queensland not-for-profit IDCARE providing cyber security learning resources and support to citizens and organisations who fall victim to cybercrime; and
- Business Queensland online information resources.

As noted above, we are surprised with the lack of incorporation of well-established and nationally accepted best practice cybersecurity framework, resources and databases from the Australian Cyber Security Centre (**ASCS**) being the Federal Government authority under the Australian Signals Directorate (**ASD**), considering same are utilised by other State Governments and operators of critical infrastructure widely across Australia.

We recommend the following is incorporated into the Cyber Plan:

(a) Information Security Manual (ISM) [2]

This is the framework produced by the ACSC for organisations to apply to protect systems and data from cyber security threats. This framework represents that considered advice of the ACSC aligned with the ASD's designated functions under s7(1)(ca) of the *Intelligence Services Act 2001* (Cth). The ISM includes the:

- Cyber Security Principles, which are grouped into four key activities: govern, protect, detect and respond[3];
- Cyber Security Guidelines which cover governance, physical security, personnel security and information and communications technology security; and
- Risk Management Framework, which has six steps: define the system, select controls, implement controls, assess controls, authorise the system and monitor the system[4]

(b) Programs

The ACSC offers training and education programs for particular sectors, such as:

(i) the Critical Infrastructure Uplift Program[5] designed to enhance the cyber resilience of Australia's critical infrastructure by:

- assist partners that own or operate critical infrastructure to better understand and improve their cyber security maturity;
- deliver vulnerability and risk mitigation recommendations; and
- increase visibility of threats to Australia's most critical systems.

As well as a Self Assessment Tool, CI-UP offers Cyber Security Posture Assessment, Cyber Security Technical Validation, Cyber Threat Hunt, Table Top Exercises, Threat Briefings and CI-UP Reporting and Debrief.

[2] Information Security Manual (ACSC): Information Security Manual (ISM) | Cyber.gov.au

[3] Cyber Security Principles (ACSC): -Cyber Security Principles | Cyber.gov.au

[4] The risk management framework used by the ISM draws from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

[5] CI Uplift Program: https://www.cyber.gov.au/acsc/view-all-content/programs/critical-infrastructure-uplift-program-ciup

(ii) the National Exercise Program[6] designed to broaden the understanding of roles and responsibilities of government agencies and private sector organisations when responding to a cyber security incident. The program uses exercises and other readiness activities that target strategic decision-making, operational and technical capabilities, strategic engagement and communications. This program is also available to owners and operators of Australia's critical infrastructure, as well as Australian, State and Territory Government organisations.

(c) Essential Eight

Significantly, the ACSC has developed the "*Essential Eight*" prioritised mitigation strategies that are well accepted as the most effective to protect organisations against various cyber threats[7]. The Essential Eight Maturity Model was first published in June 2017 and is based on the ACSC's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

(d) Cyber safety resources across industry and community

The ACSC has established practical and accessible resources for different types of business and individuals across industries. Examples include:

- Small business Cyber Guide[8];
- Spot the Spam Quiz;
- Cyber Security Assessment Tool for small/medium business;
- Personal Security Guide for individuals[9];
- step-by-step guides for individuals and families detailing basic cyber security instructions for specific software, applications and devices; and
- advice and support to Australian businesses and industry responsible for managing Australia's Critical Infrastructure and Systems of National Significance.

(e) Cyber Crime Reporting

ReportCyber is a function of the ACSC which is a national policing initiative and the first point of call for reporting cybercrime in Australia. ReportCyber refers cybercrime reports to appropriate State or Territory police for assessment.

QUEENSLAND'S CYBER SECURITY LANDSCAPE

It is also apparent that approaches to cyber security are disparate between different State Government departments. In this respect, the Cyber Plan is an opportunity to bring uniformity to practice across the State Governments, consolidate the existing initiatives without necessarily removing them and aligning practice with nationally accepted standards.

Currently in Queensland, initiatives operate across Departments/authorities that deal with different aspects of cyber security including:

- Queensland Government Information Security Policy (**ISP**)[10] applying to internal systems;

[6] National Exercise Program | Cyber.gov.au
[7] Essential Eight to ISM Mapping | Cyber.gov.au
[8] Small Business Cyber Security Guide | Cyber.gov.au
[9] Individuals & families | Cyber.gov.au
[10] https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-security-policy-is18-2018

- Queensland Police Service (**QPS**) – cybercrime reported to QPS depending on the type and severity of the incident, where the suspect is located and whether the report contains enough information about the offender;

- Queensland Government Cyber Security Unit (**SCU**) – responsible for supporting the development of the Queensland cyber security industry and local cyber security workforce as well as managing a number of whole of Government cyber security services;

- Queensland Government Customer and Digital Group – responsible for developing customer and digital strategies, policies and roadmaps along with supporting tools, standards and guides for government services.

We suggest consultation is undertaken with relevant cyber industry stakeholders as to the effectiveness of the current models and identification of challenges and opportunities to improve with a focus on adopting the ACSC best practice framework.

3. THEMES IN A REAL ESTATE CONTEXT

As noted above, we consider that consultation should be undertaken with cyber industry stakeholders as to the specific technical matters raised throughout the Consultation Paper. We do, however, provide our comments as follows on the six proposed themes which should be considered in the context of real estate businesses.

Additionally, we submit that due to the prominence and severity of cybercrime in the real estate sector as outlined below, the Cyber Plan should contain a dedicated section specifying the Department's approach to cyber awareness, security and resilience in the real estate sector and for property transactions.

In this regard, we recommend consultation to be undertaken with the REIQ on specific proposed objectives as well as the Queensland Law Society, noting that property solicitors and conveyancers are equally exposed to the risk of cybercrime in property transactions.

The following supports the strong recommendation that the real estate sector be provided with prescribed protections.

Cyberattacks in the Real Estate Industry

In recent years, cybercriminals have targeted parties to property transactions, and specifically, real estate agencies across Australia.

Real estate businesses are a lucrative target for cybercriminals due to their involvement in facilitating high-value transactions, and the level of personal information needed to be collected and stored by real estate professionals in order to carry out their obligations under the *Property Occupations Act 2014* (Qld).

The volume and frequency of funds being exchanged between parties for deposits, instalments and settlement payments make the real estate industry vulnerable to cyber-attacks; the most common being where a client, buyer or tenant receives an email they are expecting from what appears to be the real estate professional asking for funds to be transferred to a bank account portrayed to be the real estate agencies' trust account.

By way of example to illustrate the sophistication and prominence of this issue:

- In August 2022, a Queensland couple lost $39,000 when they transferred funds to a bank account believing it was the real estate agent acting in the sale of a property, after receiving a fraudulent email from a cybercriminal that had posed as the real estate agent requesting funds;[11]

- In April 2022, cybercriminals targeted a real estate business and were able to steal $52,000. The real estate agent was engaged by an elderly couple to sell their property and held the buyer's deposit, being $52,000, in their trust account. After settlement, the agent received an email from one of the sellers requesting funds to be paid to their account. However, this was a fraudulent email sent by a cybercriminal with their own bank account details. The agent transferred the funds to the cybercriminal's account. When the clients asked later when they would receive the money, the agent said they had already sent it through, and it came to light that the clients had not sent the email requesting funds;[12] and

[11] https://www.news.com.au/national/queensland/gold-coast-couple-lost-40000-in-real-estate-scam-after-buying-dream-home/news-story/e3cf8a9eb794697fa85774588c097af7

[12] https://9now.nine.com.au/a-current-affair/queensland-grandparents-hack-warning-after-real-estate-deposit-went-missing/d880daf2-2615-44c1-8c6b-89f30dbdeabb

- In early 2022, a rental property on the Gold Coast was advertised by a cybercriminal on Facebook pretending to be the letting agent. Ten people paid deposits of around $2,000 to the scammer, believing that they were securing the rental property. One person reported that they would have paid 6 months rent in advance approximating to $14,000 in order to secure the property[13].

Additionally, real estate businesses are likely to hold personal information about a high volume of individuals including their clients and other parties to property dealings such as buyers and tenants, including bank account details and forms of identification.

In November 2022, an agency fell victim to cybercriminals that were able to access the agency's database of tenant's including names, addresses, contact details, signatures and bank account details after a supplier of the real estate business was hacked after an employee used their personal phone for work purposes. The cybercriminal was able to infiltrate the system of the real estate business[14].

Unfortunately, these examples are not uncommon and illustrate the real cybersecurity risks that real estate agencies are subject to every day.[15]

The second highest category of Notifiable Data Breaches recorded between January to June 2022 was related to financial data, with the two primary sources of breach reported being malicious or criminal targeting (59%) and human error (32%)[16].

The combination of the above factors has created the ideal environment for cyber criminals to home in on unsuspecting real estate agents in their attempts to infiltrate their networks and systems.

Guidance for collecting and storing information as a real estate professional

As noted above, real estate professionals must collect particular personal information from a party in order to properly carry out their role facilitating a real estate transaction and to comply with obligations under the *Property Occupations Regulation 2014* (Qld).

Real estate professionals have both a legal obligation and a fiduciary obligation to their client, to ensure that they have:

- verified the identity of the parties to the transaction; and
- conducted adequate due diligence on a party to a property transaction.

The type of transaction and circumstances of the party may mean that different types of information must be requested.

For example:

- a business broker would need financial information and business records of a business they have been appointed to sell so that they can advertise the business and provide correct information to a prospective buyer;

[13] https://www.9news.com.au/national/scams-australia-property-real-estate-scammers-queensland/f0857824-75cd-4578-8dfa-cbe0841356c1
[14] https://www.news.com.au/technology/online/hacking/real-estate-agency-harcourts-reveals-names-addresses-possibly-compromised-in-cyber-attack/news-story/339e9bff70acf16ea12b734a4b024499
[15] https://www.9news.com.au/national/scams-australia-property-real-estate-scammers-queensland/f0857824-75cd-4578-8dfa-cbe0841356c1
[16] Notifiable Data Breaches Report Jan-June 2022: https://www.oaic.gov.au/__data/assets/pdf_file/0020/23663/OAIC-Notifiable-Data-Breaches-Report-Jan-Jun-2022.pdf

- a residential property manager would need information from a prospective tenant to determine whether they have the financial ability to meet rent and other payments without placing them in financial hardship;

- a sales agent may need identification documents from a prospective buyer when preparing a contract of sale to verify the identity of the buyer and ensure the correct legal entity is noted in the contract; and

- a buyer's agent would need to verify the identity of their client, which may include requesting directors' details or trust details if the buyer is a corporate entity.

Although real estate professionals will generally comply with obligations under Privacy Law when collecting, storing and disclosing information about a party, there can often be confusion about what information needs to actually be stored once collected and for how long. Additionally, not all real estate businesses are required to comply with privacy laws due to the $3m threshold.

With certain documents needing to be stored for a particular period under the *Property Occupations Act 2014* (Qld) and *Residential Tenancies and Rooming Accommodation Act 2008* (Qld), there is uncertainty about whether obligations apply also to personal information and in particular identity documents that are associated and verify the real estate professional's compliance with their obligations. In addition, some professional indemnity insurers require such information to be stored to document and evidence that proper steps were taken by a real estate professional in carrying out their role.

The REIQ is currently preparing an education campaign to promote best practice in the real estate profession in relation to cyber security, including promoting the deletion personal information which is not required to be stored. We suggest the Cyber Plan include consideration of various legal requirements for holding information across sectors and identify if any improvement or uniformity can be achieved through regulation.

Access to Support and Resources

As the peak body for the real estate industry, the REIQ has provided on numerous occasions, access to training, articles and best practice recommendations from cybersecurity experts to our members to educate the real estate sector about the importance of being secure and having robust systems in place to support business.

Small businesses tend to be an easier target for cyber criminals as they may not have the resources to protect their assets and data compared to larger organisations. Many small real estate businesses do not employ an internal IT specialist to assist with IT procedures and cybersecurity.

Not all business owners are technology proficient or confident with using same. At a minimum, business owners should be encouraged to engage a cybersecurity or IT specialist who can evaluate systems in place and advise on what is required to improve systems wholistically.

A potential opportunity for the Cyber Plan is to remove misconceptions around what is actually involved with becoming cybersecure as a business. The time and financial cost of implementing cyber security systems and procedures into a business, is generally much less than may commonly be believed and in this climate, is far outweighed by the benefits of doing same.

The ACSC resources for small business should be promoted for business owners who are comfortable to self-assess what they may be lacking in their systems and security infrastructure.

The Cyber Plan should also consider how to incentivise business owners to take action on this issue sooner rather than later. With this issue becoming so prominent in our society as set out in the Consultation Paper, we consider it appropriate for Government to intervene and require a minimum standard of cybersecurity to be required by businesses.

Where the cost to a business is significant, business owners may not be aware that they can access the Promoting Business Boosts Grant[17] to receive a grant payment of $15,000 for projects for the design and implementation of management systems, including:

- data warehouses;
- asset management;
- customer relationship management systems;
- risk management;
- production systems;
- project management systems;
- quality and compliance management; and
- Bespoke or complex website or application design and build, including:
  - e-commerce;
  - software integration;
  - booking systems;
  - cybersecurity tools;
  - webinar/conferencing;
  - customer accounts/logins; and
  - paywalls.

Although this grant may be appropriate for major projects, it may be too restrictive in criteria and threshold to capture lower value solutions that may be required to protect a business from cyber risks.

We recommend the Department consider if smaller grants could be made available for small businesses that need lower value solutions in order to become or improve cyber security. We consider a specific grant for real estate businesses would be advantageous given the higher risk and impact to community relating to cybercrime in the real estate sector.

The Cyber Plan should also heavily promote self-service testing and implementing resources of the ACSC. This would assist real estate professionals if they had more awareness of what they can do to train themselves and improve their cyber awareness.

Innovation and Property Technology Solutions

New technology has emerged in the property space to improve efficiency, accuracy and security of property dealings and transactions across Australia. In particular, the property technology 'proptech' industry has significantly grown in Australia over the past 5-10 years.

[17] Business Boost Grants Program | Business Queensland

In the FY21 the Australian proptech sector grew by 8.2% of companies generating over a million dollars in annual revenue. As a growing and diverse industry, new platforms and technology solutions are consistently emerging to assist real estate professionals with all aspects of their services.

Interestingly, the acceptance and adoption of technology across different States and Territories of Australia have occurred at a different rate.

As at June 2021, eConveyancing facilitated in PEXA made up 62% of property transactions in Queensland, 78% in Western Australia, 94% in South Australia, 96% in New South Wales and 98% in Victoria[18]. The figure for Queensland has since risen to 77% as at June 2022[19], being still considerably lower than other States. EConveyancing for some transactions in Queensland are only becoming mandatory as of 20 February 2023, whereas other States had mandated the practice in 2020/2021. Electronic signing also generally has more resistance in Queensland than other States and Territories in Australia.

The use of new technologies that allow for more security and certainty should be promoted in the Cyber Plan.

In our experience, real estate and property practitioners may be more resistant to using these technologies not only because they are less familiar, but also because there may be a misconception about losing the manual aspect of carrying out these services, as well as the possible disruption to business and potential costs involved.

We suggest the Cyber Plan consider options for educating business owners about the benefits of certain emerging and existing technologies in relevant sectors for business owners.

In our view, the Department can diminish resistance to these technologies by enabling easier identification of trusted secure providers and suppliers. This will benefit the industry and promote consumer confidence in new providers and suppliers, as well as assisting these businesses to develop such technologies.

Business owners that wish to adopt new technologies or find they must adopt new technologies to keep aligned with modern practice in their industry, may be more vulnerable to cybercrime if they are less confident with using the technologies. As noted above, almost a third of data breaches are caused by human error.

An opportunity may be to incentivise providers of new and established proptech to provide specialised training and education about their products to the practitioners in Queensland.

Raising Cyber Resilience

In our view, an essential element of the Cyber Plan should be broader community education about cybercrime that occurs when dealing with property as a buyer, seller, tenant or lessor.

[18] PEXA Annual Report 2021: https://investors.pexa.com.au/FormBuilder/_Resource/_module/MKCl5QLROk-78c35b6yPkA/docs/PEXA_2021_Annual_Report.pdf
[19] PEXA Annual Report 2022.

Professionals in the real estate and property industry generally have a reasonable awareness of potential risks. When acting in a real estate transaction, it is common practice for real estate professionals and conveyancing solicitors to provide warnings (both written and verbal) about the risk of cybercrime and to ensure that no funds are transferred without verifying that the person they are sending funds to is correct.

Nonetheless, with the sophistication of fraudulent emails and cybercrime methods increasing, members of the broader community are still unfortunately not as cyber-aware or resilient as they should be to protect themselves from the current cyber risks in property transactions.

Although stories as exampled above are commonly shown on social media and news outlets, there is little Government interaction on this issue within the broader community.

We recommend the Department carry out as part of the Cyber Plan, a community education campaign focused on the most prominent types of cybercrime in our society including when buying, selling and renting property, to raise awareness of how individuals can protect themselves, aligned with ACSC methodology.

Accessibility should be a key feature of such campaign, appreciating that many Queenslanders who are most at risk are also vulnerable members of our community such as the elderly, people from non-English speaking backgrounds, persons with disabilities, persons living in remote communities and alike.

For this reason, we strongly support a targeted education campaign to ensure all persons in our community have access to the information and resources they need to protect themselves against cyber threats.

4. STATE BASED CYBER STRATEGY

Most other States and Territories in Australia have a dedicated cyber security strategic plan including key objectives and deliverables set out over a specified period with regular reporting and an obvious incorporation of the ACSC best practice framework. We suggest a similar approach and model is adopted in the Cyber Plan developed by the Queensland Government.

We note the Victorian Cyber Strategy 2021[20] sets the Governments agenda for a five-year period with similar objectives to that of the proposed Cyber Plan. Importantly, this strategy recognises that critical to its success is the provision of effective resources and education across Government, industry and community sectors.

Mission Delivery Plans are released annually that outline specific activities implemented with consultation from relevant industry stakeholders. For example, the Mission Delivery 2021/22[21] identified the following deliverables:

- 19 specific targeted actions to improve visibility and risk governance of IT assets including:
  - issuing guidance on the successful implementation of the Essential Eight across government;
  - issuing Victorian Government recommended security configuration for Office365;
  - work with the National Cyber Security Committee to standardise government third party supplier security frameworks across Australian jurisdictions entities; and
  - undertake cyber education program for government executives in critical service operations.

- 7 specific targeted actions to improve understanding of cyber risks, issues and response opportunities including:
  - establishing an Expert Advisory Panel to provide insight on current and future cybercrime risks issues and response opportunities;
  - support the delivery of a new Victoria Police Cybercrime Strategy; and
  - develop an annual cyber exercise program in partnership with Victoria's critical infrastructure owners and operators.

- 13 specific targeted actions to grow cyber security skills and jobs including:
  - collaborate with AustCyber to map Victoria's cyber security ecosystem;
  - support the cyber security awareness and capabilities of SME's through Small Business Victoria's suite of support programs; and
  - explore opportunities for Victorian cyber start-ups to access developmental support and capital, through LaunchVic and Invest Victoria's suite of support programs.

An important feature of the Victorian strategic plan is the clear specification of actions and the direction set out to how the objectives will be met within the 5-year period. The strategic plan also ensures collaboration between different areas of the Victorian Government as well as incorporation of ACSC principles and Federal stakeholders. We suggest a similar, wholistic approach should be taken by the Queensland Government.

By comparison, New South Wales adopts the Essential Eight in the State's Cyber Security Policy 2021/2022[22], as well as other elements of the ISM. South Australia also has a dedicated strategy that sets out key deliverables over a 5-year period[23].

[20] Victoria Cyber Strategy 2021: https://www.vic.gov.au/victorias-cyber-strategy-2021-introduction
[21] https://www.vic.gov.au/victorias-cyber-strategy-2021-introduction
[22] New South Wales Cyber Security Policy 2021/2022 https://www.digital.nsw.gov.au/sites/default/files/2022-11/nsw-cyber-security-policy-2021-2022.pdf, New South Wales Cyber Security Strategic Plan: https://www.digital.nsw.gov.au/policy/cyber-security/cyber-security-strategy/our-strategy-at-a-glance
[23] https://www.dpc.sa.gov.au/responsibilities/ict-digital-cyber-security/ict-cyber-security-digital-strategy/ICT-Cyber-Security-and-Digital-Strategy-Update-2022.pdf

5. CONCLUSION

We strongly support the development of a robust and effective cyber security strategic plan to strengthen cyber practices, intelligence and resilience of business and the community in Queensland. This is essential to achieve the core objectives including to attract new roles, businesses and investment in Queensland, prepare a cyber workforce of the future and build infrastructure and services that are cybersecure.

It is our view that a strategic plan for cyber security in Queensland should:

- consolidate existing State and Federal initiatives and resources;
- incorporate and align with nationally accepted best practice of the ACSC; and
- introduce specific objectives and targets to achieve cyber awareness and cyber resilience in Queensland across the broader community, business and Government.

We suggest a specific focus and dedicated section in the Cyber Plan to address real estate dealings and transactions, given the prominence and severity of cyberattacks targeting real estate professionals and other property stakeholders in Queensland.

As noted, although it is commendable that steps have begun to be taken to devise the Cyber Plan, it is essential that progress is continuing for the actual development of the plan so that it may be implemented in a reasonable time.

In this regard, we suggest the development of this plan is given a high priority with a strong focus on what key deliverables are to be achieved in the Cyber Plan.

We look forward to further progress and consultation on this matter.