DLC LEGAL
PRECISION NAVIGATION

Submission to the Parliamentary Joint Committee on Intelligence and Security

Review of Cyber Security Legislative Package 2024

By DLC Legal Pty Ltd

DLC LEGAL
PRECISION NAVIGATION

Contents

About DLC Legal

DLC Legal (previously Black Ink Legal) is a boutique provider of virtual and onsite legal, strategic sourcing, procurement and contract management services to State and Commonwealth governments and private industry. Incorporated in 2021 as an Integrated Legal Practice under the banner Black Ink Legal, the firm specialises in assisting our clients to develop, structure, negotiate and manage strategically important projects and procurements through to deal completion.

DLC Legal specialises in cyber security law, and our lawyers possess a deep understanding of the complex mosaic of the cyber and technology legal landscape. Our expertise extends to advising a diverse array of clients, ranging from emerging tech startups to established multinational corporations, on a broad spectrum of cyber-related legal issues including safety-by-design, data protection and privacy, compliance with local and international cyber security standards, breach response and notification requirements, and the management of cyber risks in contractual agreements.

Our purpose is to be proactive in supporting and assisting our clients navigate the intricacies of cyber law, to safeguard digital assets and intellectual property, while ensuring their operations align with current legal frameworks. DLC Legal is passionate about and committed to ensuring robust cyber resilience, socially and structurally. Our focus is at the forefront of technological advancements and legislative changes to empower our clients to achieve their business objectives with confidence, knowing their legal exposure is minimised and their innovations are protected.

DLC Legal extends its boutique legal and strategic services to Australian managed IT providers, specialising in technical cyber support and insider threat detection technology, emphasising safety-by-design and support in privacy and cybersecurity. Our advisory services address the unique challenges faced by the IT and technology sector. We offer specialised guidance in navigating the complexities of data protection laws and cybersecurity threats. We understand the critical importance of safety-by-design, safeguarding digital assets and personal information in today's interconnected world and strongly advocate a whole of economy approach. We deliver comprehensive strategies to our clients that enhance cybersecurity measures and ensure compliance with Australian privacy laws, thereby fortifying our clients' defences against cyber threats and legal vulnerabilities.

Executive Summary

DLC Legal thanks the Parliamentary Joint Committee on Intelligence and Security to provide input into the Review of the Cyber Security Legislative Package 2024. The unprecedented maturation of artificial intelligence and by extension internet connected smart technology is changing how we live, work, and do business. It is fair to say that for the foreseeable future, we will continue to embrace the lifestyle and cultural conveniences that have developed with the evolution of these modern technologies. However, the rapid evolution of technology and uptake within society has outpaced the existing legislative framework by a significant margin. The Cyber Security legislative reform package addresses this evolving landscape of artificial intelligence and internet-connected smart technology, emphasising the need for robust security measures in connected Internet of Things (IoT) consumer devices.

DLC Legal is acutely aware that the legislative reform package will not solve all security challenges associated with IoT. There is no single standard or strategy that can protect against attacks that are prolonged or sophisticated or that require sustained physical access to a device. However, with a key focus on safety-by-design, the technical controls and organisational policies that matter most in addressing the most significant and widespread security shortcomings, the draft legislation addresses a baseline level of security, to protect against elementary attacks on fundamental design weaknesses (for example the use of easily guessable passwords) and make the provisions applicable to all consumer IoT devices. The legislation should be complemented by other standards (for example AI, data protection etc) and standards that define more specific provisions and fully testable and/or verifiable requirements for specific devices.

Exposure Draft Cyber Security Bill 2024

The Exposure Draft Cyber Security Bill 2024 introduces comprehensive measures to enhance cyber security across various sectors in Australia. While the draft Bill aims to address critical areas such as secure-by-design standards for Internet of Things (IoT) devices, ransomware reporting obligations, and the coordination of major cyber security incidents, it also introduces several risks and issues that need careful consideration.

Broad Definitions and Scope

The definitions of key terms like “cyber security incident” and “relevant connectable product” are broad and could lead to overreach and unintended application of the law, affecting entities not originally intended to fall under the regulatory scope. Consider narrowing these definitions to ensure only the intended entities and incidents are covered, possibly by providing more specific examples or criteria. That said, we feel strongly that electric vehicles and vehicles that are connected to the internet by design should be included in the definition of ‘relevant connectable product’.

Compliance Burdens

The draft Bill places significant compliance obligations on manufacturers and suppliers of IoT devices, including adherence to security standards and provision of compliance statements. Smaller businesses might find it challenging to meet these requirements, which could stifle innovation and competition. We recommend a phased compliance timeline. Additionally, consider offering support or exemptions for small and medium-sized enterprises (SMEs).

Enforcement Mechanisms

The enforcement mechanisms, including compliance notices, stop notices, and recall notices, are stringent and may lead to severe penalties. This may create a risk of disproportionate and potentially overly punitive penalties for minor infractions. We recommend implementing a tiered penalty system that scales penalties based on the nature, severity *and* intent of the infraction. Consider also a grace period for first-time offenders as a way to introduce corrective measures prior to facing severe penalties.

Reporting Burden for Ransomware Payments

The Bill mandates reporting of ransomware payments within 72 hours. While businesses might be overwhelmed by what could be considered a short reporting window, there is a low risk that this could lead to underreporting or non-compliance. However, in our view, any mandatory reporting of ransomware payments could be made on or around the same time as the ransomware payment. Once the payment is made the longer an entity takes to report that payment the less likely authorities are able to assist the affected organization. A more pressing concern in our view is to consider whether ransomware payments should even be made at all. The premise of a mandatory reporting regime implies that it is acceptable and appropriate to make ransomware payments. This in turn risks setting up a regime where a culture of paying ransomware is considered routine. We consider an appropriate approach would be one which deters organisations from making ransomware payments, but in scenarios where they do, then they must report those payments. It is worth noting that in many cases where payments are made, the data is not provided by the hacker or is provided but is severely compromised.

Additionally, there are concerns with respect to cyber threat intelligence sharing. It goes without saying that all critical infrastructure entities need to be proactive with cyber security measures. It follows therefore that all entities responsible for critical infrastructure should be included and by extension, cyber threat intelligence sharing between critical infrastructure entities should be required.

Privacy Concerns and Data Storage

Many consumer IoT devices and their associated services process and store personal data. The draft Bill allows for the collection and sharing of significant amounts of data, including potentially sensitive information. This risks potential privacy breaches and misuse of data if not properly safeguarded. It is vital that appropriate guardrails are implemented, for example through strengthened data protection measures, including encryption and access controls and requirements that data sharing is limited to the minimum purpose necessary and is the process is transparent. That said, we observe that the while the draft Bill does not explicitly reference the General Data Protection Regulation (GDPR) 2016, there are several provisions that align with principles found in the GDPR, particularly those related to data protection and privacy. Future iterations of the draft Bill should take into consideration the interplay with international data protection legislation including the *General Data Protection Regulation 2016* where Security-by-Design is an important principle.

Coordination and Information Sharing

The draft Bill encourages voluntary information sharing with the National Cyber Security Coordinator. Noting the voluntary nature of this requirement, there might still be reluctance from businesses to share information due to concerns over confidentiality and potential liability. However with clear legal protections for entities sharing information in good faith and the implementation of appropriate safeguards, shared information should be mandated, under strict legislated conditions and used strictly for permitted purposes. That said, we question the long term effectiveness of voluntary information sharing and suggest that reporting of certain cyber security information should be mandated in certain circumstances. Tied to this, we note the importance of enforcement. Entities must not be exempted

from their cyber security obligations, including reporting obligations. It is of paramount importance that legislative and regulatory obligations be enforced.

Operational Independence of the Cyber Incident Review Board (CIRB)

While the CIRB is given independence under the draft Bill, the requirement for Ministerial approval of the terms of reference for a review by the CIRB risks undermining the public perception of this independence. This in turn could lead to perceptions of political influence. Ministerial oversight is an important aspect of our country's governance, however not every incident is created equal and not every review will be so severe as to warrant Ministerial oversight of that review's terms of reference. Accordingly, we encourage limiting the requirements for Ministerial approval to exceptional circumstances. Such exceptional circumstances might need to be defined in the draft Bill, but this would allow the CIRB greater flexibility and autonomy. We also support a no-fault principle approach in order to ensure true stakeholder engagement. We support the inclusion of a variety of stakeholders in post incident review sessions. In particular, we support a national instrument to represent the interests of the entire community (government, individuals, businesses, schools, hospitals etc) to provide effective and truly representative examination of the technical severity and complexity of a given incident, including the impact on national security, social and economic consequences, and impact on the broader community.

Impact on International Relations

The extraterritorial application of the draft Bill could affect international entities doing business in Australia and potentially risks conflict with the laws of other jurisdictions. While this could cause diplomatic issues and complicate international trade and cooperation, alignment of the draft Bill with applicable international standards and appropriate international partners will ensure these risks are mitigated.

Security Standards for a Relevant Connectable Product

The draft Bill addresses compliance with security standards for a relevant connectable product. It is not immediately clear which specific security standard is being referred to in this section. We note that at recent closed town Hall hosted by the Department, 'Standards' are to be created by Ministerial power under the legislation. We seek clarification whether these Standards are the same standard to which section 14 of the draft Bill refers? In addition, in creating these standards, to what extent will the Bill draw on international frameworks where more established, relevant cyber security standards exist—For example, alignment with the ETSI EN 303 645 as well as broader international industry standards in addition to creating bespoke standards under the new powers contemplated by the draft Bill? Will these standards include security standards for electric vehicles and vehicles with in-built 'smart-systems' that connect these vehicle to the internet. The connectivity capability of most modern vehicles puts them at as much if not greater risk as all other 'relevant connectable products' and accordingly, should be considered within this reform package.

Exposure Draft- Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024

The *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024* (the Exposure Draft) proposes several key changes and obligations which improve on the existing *Security of Critical Infrastructure Act 2018* (the SOCI Act) including:

Inclusion of Data Storage Systems Holding Business Critical Data

The Exposure Draft adds a new subsection to the SOCI Act that considers data storage systems holding business critical data as part of the critical infrastructure asset. This means obligations under the Act, such as risk management programs and notification of cyber security incidents, will also apply to these data storage systems. Holding the critical data of a business recognises the importance of that data and the business in the critical infrastructure ecosystem. Further, the Exposure Draft mandates that critical infrastructure risk management programs must now also cover data storage systems that hold business-critical data. We note that this expansion acknowledges the increasing importance of data systems in the context of critical infrastructure security. Consider adding explicit obligations on data storage systems and providers of data storage systems stating that they are not exempted from their cyber security obligations, including reporting obligations.

Expanded Scope of Incidents

The Exposure Draft replaces references to "cyber security incidents" with "incidents" (including cyber security incidents). We support this broadened scope as it will also include non-cyber security incidents that may impact critical infrastructure assets.

Ministerial Authorisation for Responding to Serious Incidents

The Exposure Draft introduces a new regime where the Minister may authorise the Secretary to issue information-gathering directions, action directions, and intervention requests to relevant entities to respond to serious incidents impacting critical infrastructure assets. This provides a structured approach to mitigate the consequences of such incidents. The Exposure Draft also allows the Minister to issue directions regarding risk management programs in response to serious incidents. This includes the authority to direct entities to modify their risk management strategies to address specific threats or vulnerabilities identified during incidents.

Disclosure of Personal Information

The Exposure Draft allows the Minister to authorise the disclosure of personal information held by entities to other entities for specified purposes when responding to serious incidents. This can mitigate risks involved with serious incidents provided that specified purposes are clear and relevant to mitigating a serious incident(s). We refer to previous recommendations in this submission where we question the long term effectiveness of voluntary information sharing and suggest that reporting of certain cyber security information should be mandated in certain circumstances. Ministerial mandate may go some way to alleviating these concerns where serious incidents are concerned. That said, there are times

when a minor incident may turn into a serious incident and could be mitigated with a robust information sharing scheme between entities responsible for critical infrastructure.

Expanded Definition of Protected Information

The Exposure Draft expands the definition of "protected information" to include documents or information obtained, generated or adopted under, or relating to the operation of, the Act. This will hopefully ensure that a wider range of sensitive information is safeguarded.

Exposure Draft – Intelligence Services and Other Legislation Amendment (Cyber security) Bill 2024

The exposure draft of the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024 (the Exposure Draft), proposes several key improvements to the *Intelligence Services Act 2001* (the ISA). In particular, the Exposure Draft's enhanced Cyber Security focus, significantly improves the ISA's ability to address modern cyber security challenges. Specifically, the Exposure Draft introduces several notable improvements to enhance cyber security information sharing and management. By providing protections for information shared on a voluntary basis, the draft aims to encourage entities to be more forthcoming with details about cyber security incidents. This approach may foster a more open and collaborative environment for addressing cyber threats.

Additionally, the draft offers clearer and more detailed definitions of cyber security incidents and permitted purposes, which provides greater clarity for all parties involved in the process. This increased precision in terminology can help reduce ambiguity and improve understanding among stakeholders. Furthermore, the exposure draft strives to strike a balance between the need for information sharing and the importance of privacy and legal protections for individuals and entities. This balanced approach demonstrates an effort to address the complex challenges of cyber security while respecting individual rights and organisational interests.

Concluding thoughts and Recommendations

Draft Cyber Security Bill

The draft Bill addresses critical areas of concern in the modern digital landscape. However, it introduces several significant risks and issues that need to be considered, to ensure its effectiveness and fairness. By refining definitions, easing compliance burdens, ensuring proportional enforcement, safeguarding privacy, enhancing coordination mechanisms, and maintaining operational independence, the draft Cyber Security Bill will achieve its objectives while minimising unintended, adverse consequences. That said, it is essential to establish clear guidelines and thresholds that define what constitutes a "serious incident." This will ensure a consistent application of the new response regime across various sectors. Second, robust oversight mechanisms and accountability measures are recommended to govern the use of Ministerial authorisations. This will ensure public trust and mitigate the risk of misuse (real or perceived, inadvertent or otherwise), or overreach in the exercise of these powers. Additionally,

implementing stringent data protection and privacy safeguards is crucial when personal information is involved. This step will mitigate potential privacy risks associated with the sharing of sensitive data during incident responses.

Draft Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024

Training and resources are vital. We recommend providing training support to entities to assist in adapting to the new legislative environment, particularly concerning the integration of data storage systems into their risk management programs. We also encourage the implementation of a framework for regular review and updates of risk management programs to enable entities to remain aligned with evolving threats and regulatory requirements, to enhance the resilience of critical infrastructure in the face of emerging challenges.

Draft Intelligence Services and Other Legislation Amendment (Cyber security) Bill 2024

The exposure draft tackles the ever evolving, ever increasing threat of cyber security challenges through the provision of a clear framework for handling cyber security information. We are encouraged by the enhanced framework that incentivises information sharing by providing protections for voluntarily shared information. The detailed definitions of cyber security incidents and permitted purposes provide greater clarity for all parties involved, while attempting to balance the need for information sharing with privacy and legal protections for individuals and entities. That said, in the spirit of continuous improvement, enhanced transparency, accountability, and effectiveness we make the following recommendations to safeguard appropriate and effective application of the new powers to ensure that the legislative framework remains relevant and effective in the rapidly evolving cyber security landscape. These include adding a provision for regular review of the effectiveness of these new measures, considering international cooperation provisions, including specific protections for whistleblowers, and adding provisions for creating public awareness about cyber security threats and best practices. Other potential improvements might include specifying maximum retention periods for cyber security information, strengthening oversight provisions, and providing more specific criteria for determining what constitutes an "imminent risk" in the context of cyber security incidents.

There is no silver bullet that will combat the ever-increasing threat of cyber security incidents, but the recommendations in this submission aim to enhance transparency, accountability, and effectiveness of the new cyber security provisions while maintaining a balance with national security needs. Looking forward, the draft legislative package clearly seeks to bring together best practice security for IoT consumer devices in a set of outcome-focused provisions that support all parties involved in the development and manufacture of consumer IoT with a robust and pragmatic guidance on securing their products. Generally speaking, the draft legislation appears outcome-focused, giving organisations the flexibility to innovate and implement security solutions appropriate for their products.

The promotion of secure-by-design principles, fostering collaboration across stakeholders, and establishing mechanisms like the CIRB for incident review and policy guidance, aims to enhance national cybersecurity resilience and underscores the importance of continuous improvement, stakeholder engagement, and adherence to best practices to create a safer digital environment for all Australians. The focus on technical controls and organisational policies is crucial in addressing significant security shortcomings, but it is imperative to recognise that sophisticated attacks and evolving threats may require continuous adaptation and vigilance. The interplay with data protection legislation, alignment with related standards, and considerations for evolving technologies will be key factors in shaping a robust legal framework for cybersecurity in IoT devices. By promoting secure-by-design principles, fostering collaboration across stakeholders, and establishing mechanisms like the CIRB for incident review and policy guidance, national cybersecurity resilience underscores the importance of continuous improvement, stakeholder engagement, and adherence to best practices to create a safer digital environment for all Australians.

DLC Legal welcomes the release of the next iteration of the draft legislation and round of consultation.

Melanie Hutchinson
Special Counsel, DLC Legal
[redacted]