CISO LENS

Submission to Parliamentary Joint Committee on Intelligence and Security

Cyber Security Legislative Reform Package

October 2024

24 October 2024

cisolens.com
ABN: 54 613 115 290

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Committee Secretary

Submission to Inquiry on Cyber Security Legislative Reform Package 2024

CISO Lens welcomes the opportunity to make this submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry regarding the Cyber Security Legislative Reform Package 2024.

CISO Lens is the strategic information sharing and analysis community (ISAC) for cyber security executives from the largest organisations in Australia and New Zealand. Our community comprises more than 70 of the largest organisations in Australia, equating to about 54 per cent of the total market cap of the ASX100. Most of our members are considered critical infrastructure and essential services, and collectively employ more than 6,500 security professionals, mainly in Australia and New Zealand. We are making this submission because our mission is to support the cyber resilience of Australia and New Zealand.

The enclosed submission presents the views of CISO Lens and is informed by regular discussion with our members about the Cyber Security Reform Package.

Should you have any questions regarding our submission, please contact David Cullen, Director of Cyber Advocacy and Uplift, [redacted]

Kind Regards,

[redacted]

James Turner
Founder and Managing Director

Context

On 9 October 2024, the Hon Tony Burke MP wrote to refer the Cyber Security Legislative Package to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for inquiry and report.

The Cyber Security Legislative Package 2024 intends to implement seven initiatives under the 2023-2030 *Australian Cyber Security Strategy*, which aims to address legislative gaps to bring Australia in line with international best practice and help ensure Australia is on track to become a global leader in cyber security.

These measures, which are captured via the Cyber Security Bill 2024 and the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024, are intended to address gaps in current legislation to:

- mandate minimum cyber security standards for smart devices,
- introduce mandatory ransomware reporting for certain businesses to report ransom payments,
- introduce 'limited use' obligations for the National Cyber Security Coordinator and the Australian Signals Directorate (ASD), and
- establish a Cyber Incident Review Board.

The Cyber Security Legislative Package also intends to progress and implement reforms to the *Security of Critical Infrastructure Act 2018* (SOCI Act). These reforms intend to:

- clarify existing obligations in relation to systems holding business critical data,
- enhance government assistance measures to better manage the impacts of all hazards incidents on critical infrastructure,
- simplify information sharing across industry and Government,
- introduce a power for the Government to direct entities to address serious deficiencies within their risk management programs, and
- align regulation for the security of telecommunications into the SOCI Act.

This submission by CISO Lens deals with the four elements listed above regarding the Cyber Security Bill 2024 and the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024, and the enhanced government assistance measures featured in the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024.

About CISO Lens

CISO Lens is the premier information sharing and analysis community for cyber security executives from the largest organisations in Australia and New Zealand.

Our mission is to support the cyber resilience of Australia and New Zealand. We work toward this mission through:

- Peer networking
- Structured collaboration
- Information sharing
- Community coordination and analysis, and
- Benchmarking.

A key driver for the creation of CISO Lens was the recognition that cyber risk is a business issue that can be most effectively addressed through collaboration across organisations and industries.

Profile of CISO Lens' member organisations

CISO Lens is designed for very large ASX/NZX companies, critical infrastructure providers, and large government departments. These organisations have the largest numbers of staff, the most complex environments, and support millions of customers and citizens.

CISO Lens' member organisations collectively:

- Represent ~54 per cent of the total market cap value of the ASX All Ordinaries Index
- Have a combined annual security budget of $2.7 billion, representing about 35 per cent of security spend in the Australia and New Zealand region, and
- Employ more than 6,500 security professionals across Australia and New Zealand, and other nations.

It is important to note this submission presents the view of CISO Lens (the organisation) and is informed by regular discussion with our members about the proposed cyber security reforms.

In addition to advocating for the interests of our members, where necessary we also present issues and implications for the wider community, in the spirit of supporting improved national cyber resilience for all Australians.

As CISO Lens does not publicly acknowledge the identity of its member organisations (to enable them to speak openly about security and risk management issues), members' views have been both anonymised and aggregated for the purpose of inclusion in this submission.

CISO Lens' views on the Cyber Security Legislative Reform Package

Since the introduction of proposed cyber security reforms by the Department of Home Affairs in late 2023, CISO Lens and its members have maintained a keen interest in the evolution of the legislative package.

CISO Lens made a formal submission to the Department of Home Affairs in February 2024, in response to its call for public feedback on the 2023-2030 Australian Cyber Security Strategy Legislative Reforms.

Consistent with our earlier submission to the Department of Home Affairs, our submission to the PJCIS is informed through regular discussion with our members about the proposed reforms, drawing on their extensive experience in managing cyber risk for large and complex organisations operating across Australia and overseas.

Overall, CISO Lens supports the introduction of new legislation to:

- mandate minimum cyber security standards for smart devices,
- introduce mandatory ransomware reporting for certain businesses to report ransom payments,
- introduce 'limited use' obligations for the National Cyber Security Coordinator and ASD, and
- establish a Cyber Incident Review Board.

CISO Lens asserts these legislative measures will have a positive impact on Australia's overall cyber resilience, by improving our understanding of the national threat picture and our operational / strategic response needs, while also better protecting new and emerging technologies against an evolving threat landscape.

However, CISO Lens holds a level of concern about the enhanced government assistance measures featured in the proposed SOCI Act amendments. While the adoption of an all-hazards approach to the direction powers is broadly supported, we are concerned the proposed legislation lacks financial assistance measures for organisations that incur costs as a result of complying with a government directive.

Although the legislation is only ever intended to be used as a 'last resort' and provides multiple safeguards for the use of the directions powers, the absence of financial assistance provisions and other protections for organisations that incur costs or other adverse impacts as a result of complying with a government directive exposes our member organisations to potentially significant risks.

Mandating minimum cyber security standards for smart devices

CISO Lens supports the introduction of mandatory minimum standards for smart devices. Just like the introduction of minimum safety standards for cars and other vehicles to ensure that drivers and passengers are provided with a minimum level of safety when on the road, we assert the introduction of minimum cyber security standards for smart devices is a positive step toward keeping Australians safe when they connect their devices online.

CISO Lens members regularly express their desire for governments to be bold and clear in their expectations about cyber security, often preferencing mandatory standards over voluntary codes. With clear mandates in hand, our members can agitate for the organisational resources and support they need to ensure compliance, thereby delivering better community security outcomes than can be otherwise delivered via voluntary codes (which can be quickly deprioritised when resources are challenged).

Subject to passage of the legislation, CISO Lens encourages the Department of Home Affairs and other relevant government entities to work closely with Australia's cyber security community to support the effective implementation of the policy. This includes consultation with IOT cyber security experts to identify and prioritise the subset, type, and classes of devices to be subject to mandatory security standards, with consideration given to the risk to device users, the current ease of compromise, and the likely effectiveness of new security controls.

Introducing mandatory ransomware reporting for certain businesses to report ransom payments

CISO Lens supports the introduction of mandatory reporting of ransom payments for businesses generating annual turnover of greater than $3 million. We assert this is an important step toward building an enhanced national picture of the ransomware problem, to support targeted law enforcement action and international action that disrupts the organised cybercrime groups targeting Australia's largest and most critical organisations.

CISO Lens members that have experienced major ransomware incidents speak positively about their interactions with Australian law enforcement. Our members have been impressed with the results generated by joint ASD and law enforcement Taskforce Aquila, which was established to investigate, target and disrupt cybercriminal syndicates, with a priority on ransomware threat groups. Taskforce Aquila's efforts to identify, investigate and disrupt offshore ransomware operators, including through its global law enforcement partnerships, have sent a clear message to the global cybercrime community that Australia will respond to serious breaches with significant force.

CISO Lens supports the intention of the legislation to capture information from ransomware victims about the type of ransomware used, the vulnerabilities that are being exploited, and the overall impact

of an incident. Capturing this data will contribute to a rich national picture of the ransomware problem. However, it is important to note these details will not always be known by victims, particularly when a victim is of low cyber maturity, or at the early stages of a forensic investigation. CISO Lens asserts the absence of this information should not be treated as a failure to fulfil the reporting obligations.

Regarding implementation of the new reporting obligations, CISO Lens supports the adoption of a transition period of 6-months before enforcement of the new requirements takes effect, to ensure that industry has adequate time to implement the reforms (as outlined in the Explanatory Memorandum).

Introducing 'limited use' obligations for the National Cyber Security Coordinator and the ASD

CISO Lens supports the introduction of a legislated limited use obligation for ASD and the National Cyber Security Coordinator, as set out in the Cyber Security Bill 2024 and the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024. Our members tell us they want to share information openly with ASD within minutes of identifying a potential incident, with the explicit guarantee that information will not be shared publicly, nor feature in any regulatory action.

In March 2023 CISO Lens surveyed its members on their perceptions of limited use arrangements for cyber security incident reporting to ASD. The survey found that while most members reported there were operational and intelligence benefits to engaging with ASD, timely information sharing with the agency (particularly with its Australian Cyber Security Centre group) was inhibited by perceptions of it being too close to the Department of Home Affairs (as the cyber and critical infrastructure regulator), and the absence of clearly defined and documented limited use arrangements.

CISO Lens members regularly express concern that, in the absence of any legislative protections, information they share with ASD and the National Cyber Security Coordinator will be shared with Commonwealth Government regulators. Our members are concerned that regulators will use this information to initiate new investigations, or hold that information for use against their organisations in future regulatory actions. These concerns are almost certainly a key driver for the plateau in reporting observed by ASD, as noted in the Explanatory Memorandum.

With the right limited use arrangements in place, Australian enterprises will be more confident to share with ASD and the National Cyber Security Coordinator, providing more detail and acting faster than we have seen before. These conditions are essential to develop the longer term 'muscle memory' that we need for Australia so that when a wide-scale and potentially nation impacting incident occurs, the habits of effective sharing are already in place.

This established cadence of fast and fulsome information sharing will be crucial in maximising the national response and reducing adverse impacts to the community. Without these arrangements in place, Australia will lack a pivotal piece of its overarching cyber capability.

Establishing a Cyber Incident Review Board

CISO Lens supports the establishment of a Cyber Incident Review Board (Board) to provide independent, objective and no-fault reviews of cyber incidents impacting Australia. It is important that Australia consider both its preparedness for, and the effectiveness of its response to, cyber security incidents to identify opportunities to enhance its national cyber resilience.

CISO Lens members have expressed a strong desire to see the Board operate in an impartial manner, and with the requisite expertise to enable timely and meaningful review and reporting on issues relating to the management of cyber security incidents.

In this context, our members have expressed concern in three key areas:

- Persons selected for the expert panel, which will support the Chair and standing members in understanding the complexities of cyber security risk, must be genuine subject matter experts with lived experienced in their related domain(s). Concern exists that if the subject matter experts bring more opinion and theory than hands-on experience, this could undermine both the credibility and effectiveness of the Board's work.
- The Board must conduct reviews and present actionable insights in a timely manner. CISO Lens members want to see the Board move quickly to initiate and undertake its reviews of major incidents, and share timely findings that help government and industry organisations enhance their cyber defences and incident management arrangements. Put another way, if the Board is slow to act and unhurried in its reporting, it risks losing credibility and relevance with the cyber security community.
- Managing conflict of interest risks for the Chair, standing members and the expert panel will be central to the credibility of the Board and the appetite of private industry to accept the findings and recommendations of its reviews. Concern exists that, without proper conflict of interest arrangements, Board participants with actual, potential or perceived conflicts of interest, including their financial interests and personal relationships, may allow these interests to influence their actions or decisions in relation to the Board's work.

Should the Bill pass into legislation, CISO Lens and its members would welcome clear advice and transparency from government about the process involved to select the Board Chair, standing members and expert panel, and detail about the arrangements in place to effectively manage conflict of interest risks.

Enhancing government assistance measures to better manage the impacts of all hazards incidents on critical infrastructure

CISO Lens supports in-principle the adoption of an all-hazards approach to government assistance measures. We acknowledge the government's desire to have the tools necessary to effectively manage major incidents, particularly those impacting multiple sectors simultaneously, to reduce impacts and harms to communities. However, we are concerned the legislation exposes our members' organisations to a variety of financial and commercial risks, for which the legislation provides no avenues of recourse.

CISO Lens is concerned the proposed legislation does not contain any financial assistance measures for organisations that incur costs as a result of complying with a directive issued by government, potentially exposing our members' organisations to significant financial costs. As one member posed: *'If we are directed by government to turn off machine x, and the cost of restoring that machine to normal operation post-incident is significant, will government cover the associated costs? These are costs that would otherwise not exist for us.'*

Similarly, CISO Lens members have expressed concerns about other risks and issues that might arise as a result of complying with a government directive. For instance, several members posed a scenario whereby complying with a government directive to modify how a particular system or service operates could void their insurance policies. Members also posed a scenario where being directed by government to modify or redirect essential services could have other, unintended consequences for the community that result in serious harm (e.g., environmental damage or threat to life).

Our members are eager to see the government provide organisations that comply with a directions power with a level of protection against commercial or other adverse consequences that arise.

Although the Department of Home Affairs has emphasised in its discussions with CISO Lens the various safeguards that exist in legislation before a directions power can be issued, including activation thresholds and the factors a Minister must consider, we remain concerned the current approach does not do enough to protect organisations against adverse financial, commercial or other outcomes.

Final observations

The 2023-2030 *Australian Cyber Security Strategy* sets the bold and entirely appropriate ambition of seeing Australia become a world leader in cyber security by 2030. For Australia to realise this goal and maximise the economic, social and other benefits the Internet and digital technologies provide, we must continually strengthen our national cyber resilience and ensure that we are prepared to respond effectively to, and recover quickly from, any risks that emerge.

Effectively managing our national cyber risk requires close partnership between the government and private industry. While government sets policy and regulates compliance with relevant legislative requirements, many of the systems and datasets that support our communities are owned and operated by private industry.

CISO Lens asserts it is essential that cyber security risk management policies set by government are both informed by industry, as practitioners and those principally charged with adopting them, and challenge industry to continually raise the bar in enhancing their cyber defences.

Acknowledgement

CISO Lens thanks the Department of Home Affairs and its senior officials for its regular and constructive engagement with its members throughout the consultation process in support of this reform package.

CISO LENS