29 February 2024

CISO Lens Pty Ltd
PO Box 6406
North Sydney, NSW 2059
Australia
www.cisolens.com

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Response to consultation on the 2023-2030 Australian Cyber Security Strategy Legislative Reforms

CISO Lens welcomes the opportunity to provide feedback on the 2023-2030 Australian Cyber Security Strategy Legislative Reforms.

This topic is of significant interest to CISO Lens and its members. Our community comprises more than 70 of the largest organisations in Australia, equating to about 40 per cent of the total market cap of the ASX100. Most of our members are considered essential services, and collectively employ over 5,000 security professionals. Our shared mission, above all, is to help make Australia a more cyber secure nation.

We thank the Department of Home Affairs for engaging early with our community on these important reforms. The town hall session you hosted on 5 February 2024 was well-attended by our members, who valued the opportunity to discuss the proposed reforms with your officials.

Our feedback is informed through 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. Our feedback addresses four of the measures featured in the consultation paper:

- Measure 2 – Ransomware reporting for businesses
- Measure 3 – Limited use obligation
- Measure 4 – A cyber incident review board
- Measure 6 – Consequence management powers.

You can find our feedback on these proposed reforms in the enclosed paper.

A common theme to emerge during our discussion with members was a concern that government is creating an increasingly complex web of cyber security, privacy and data protection legislation and regulation for Australian companies to follow. Our members expressed strong desire to see government harmonise existing legislation and regulation, integrated with any new obligations. We encourage the department to consider this feedback alongside the commentary provided on the four reform measures.

Thank you again for the opportunity to provide feedback on the Consultation Paper.

If you have any questions or would like to discuss any aspect of this feedback, please feel free to contact me directly via email to [removed] or on [removed].

Kind Regards,

David Cullen
Director Advocacy and Uplift
CISO Lens

FEERBACK ON PROPOSED REFORMS

Measure 2: Ransomware reporting for businesses

CISO Lens supports in-principle the introduction of a mandatory, no-fault, no-liability ransomware reporting obligation for Australian businesses to report ransomware incidents and payments, where doing so supports targeted law enforcement action and national action that disrupts the organised cybercrime groups targeting Australia's largest and most critical organisations.

CISO Lens asserts that any new mandatory ransomware obligation should:

- Align with the scope and impact thresholds for mandatory Cyber Security Incident Reporting contained in the SOCI Act, to enable high-value information collection and avoid capturing reports about no- or low-impact ransomware and extortion events.
- Integrate with the forthcoming legislative limited use arrangements for the Australian Signals Directorate (ASD) and National Cyber Security Coordinator, with the no-fault and no-liability protections enshrined in legislation. Reports made to ASD about ransomware and cyber extortion incidents (and any related payments) should receive the same information sharing and use protections as other cyber incident reports.
- Limit the scope of additional information required to be reported by organisations to only what is most necessary to build an improved national threat picture and support enhanced law enforcement responses—such as information about the variant of ransomware used (if known), the nature of communications with the cybercriminals (if applicable), initial access techniques (if known) and business impacts—to balance government's information needs against entities' capacity to fulfil the reporting obligation. The priority for victim entities should always be responding to the incident itself, rather than capturing volumes of data for future analysis by government.
- Feature civil penalty provisions (as part of a compliance framework), rather than a criminal penalty.

<u>Scope the scheme</u>
The consultation paper asserts the scheme is intended to help government build an improved national picture of the ransomware problem and help law enforcement agencies move faster to stop cyber criminals.

We acknowledge that applying the scheme to all entities with an annual turnover of more than $10 million, as is considered in the consultation paper, would greatly increase the size of the dataset available to government to build a national picture of ransomware, and generate more law enforcement referrals.

However, we believe the intended outcomes of the scheme could instead be achieved through greater promotion of the existing Report Cyber portal and use of the forthcoming limited use obligation for ASD. This would avoid the need to create new regulatory obligations for 42,000 Australian businesses (many of which have limited cyber capacity and capability), while also avoiding the need to establish and resource the the related industry education and regulatory compliance program.

<u>Sharing ransomware information</u>
Information collected by government about ransomware and cyber extortion incidents should be shared publicly, in anonymised form, via the annual ASD Cyber Threat Report. This report

is already well recognised by private industry as a trusted source of authoritative advice on current and emerging cyber risks and issues. It is an invaluable form of evidence-based decision support for executives who may not be fully across the challenges of conducting business online.

In addition to reporting on ransomware trends and insights, government should also showcase stories of successful law enforcement disruptions and prosecutions arising from reported incidents, to demonstrate how information gathered via the scheme is used by government to reduce the risk of cybercrime in Australia.

Measure 3: Limited use obligation for the Australian Signals Directorate and National Cyber Security Coordinator

CISO Lens supports the introduction of a legislated limited use obligation for ASD and the National Cyber Security Coordinator. Our members want to share information openly with ASD within minutes of identifying a potential incident, with the explicit guarantee that information won't be shared publicly, nor feature in any regulatory action.

In March 2023, we surveyed our members on their perceptions of limited use arrangements for cyber security incident reporting to ASD. The survey found that while most members believed there were operational and intelligence benefits to ASD obtaining formalised safe harbour status, timely information sharing with the agency was currently inhibited by perceptions of it being too close to the Department of Home Affairs (as a key regulator), and the absence of clearly defined and documented limited use arrangements.

CISO Lens asserts that for any limited use arrangements to be effective, it is essential to provide explicit safeguards regarding the sharing of information with, and use of information by, regulatory bodies. This is considered non-negotiable by our members, who are concerned that without the appropriate safeguards in place, information shared with ASD under limited use arrangements may serve as a trigger for, or form part of, formal regulatory action (through either domestic or international regulatory bodies).

To address this concern CISO Lens recommends the legislation explicitly assert that:

- the provision of information to ASD under limited use arrangements does not in itself constitute a regulatory notification;
- any information obtained by ASD under limited use arrangements and shared with a third-party can only be used for the prescribed purposes (aligned to those contained in the recently circulated draft Statement of Comfort); and
- regulators cannot use information obtained from the ASD under limited use arrangements to commence, or form part of, any formal regulatory action.

With the right limited use arrangements in place, Australian enterprises will be more confident to share with ASD, 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 for ASD, Australia will lack a pivotal piece of its overarching cyber capability.

Measure 4: A Cyber Incident Review Board

CISO Lens supports the establishment of a new national cyber incident review board, to identify and share lessons learned from Australia's handling of nationally significant cyber incidents, and to make recommendations to help improve our national cyber resilience.

Our members have expressed the view that for entities to be encouraged to participate in the review process, and for the mechanism to have a meaningful impact, a new cyber incident review board should:

- Examine nationally significant cyber incidents, determined by the scale of impact and/or the potential to identify opportunities to enhance Australia's national cyber incident response capability.
- Focus on strategic trends, risks and issues relevant to Australia's national cyber incident response capability. There is strong desire to see the review board examine issues of strategic governance, coordination and engagement, information sharing, public information, and community relief and recovery.
- Avoid being drawn into the realm of operational intelligence sharing, which should remain the domain of ASD.
- Operate on an impartial, no-fault basis, avoiding attribution of fault or public criticism of entities that experience a cyber incident.
- Comprise members who are cyber security subject matter experts, in particular those with extensive experience in cyber security and strategic risk management, major incident management, and/or system-level assurance reviews.
- Be supported by an expert advisory body made up of independent, technical subject matter experts who can advise the review board on highly complex technical matters relevant to their reviews.
- Preclude membership from persons holding a financial interest in the sale of cyber security goods and services, who may seek to, or be perceived to, benefit from their involvement in the review board. The management of conflicts of interest will be, in our opinion, critical to building and maintaining industry trust in the review board.
- Feature an independent chair who is highly respected and well-regarded across Australia's cyber security community, who has an appreciation for the workings of both private industry and government, and who can provide a clear and trusted voice to government, industry and the community on opportunities to strengthen Australia's cyber security resilience.
- Establish and publish clear terms of reference for each review, with reviews self-initiated by the chair or at the request of the Minister for Cyber Security.

Measure 6: Consequence management powers

Following careful consideration of information currently available through the consultation paper and discussion with department officials during the townhall sessions, CISO Lens does not support the proposed introduction of new consequence management powers.

While we acknowledge the issues raised in the consultation paper, in particular the data sharing challenges faced by Optus and Medibank in 2022 and commend the government's desire to continually improve consequence management outcomes for the Australian

community, our members are concerned the proposed reforms are disproportionate to the problems they seek to address.

Our members cite a range of existing legislative mechanisms, sector forums and engagement channels available to government at both the state and federal level, operating within and across sectors, to help manage the consequences of major incidents and emergencies.

We welcome further advice from the department that would provide evidence of the need for new legislative consequence management powers, including real-world case studies that demonstrate where existing legislative mechanisms, sector forums and engagement channels failed to achieve the desired consequence management outcomes.