Cyber Security Legislative Reforms

- Rules and Implementation Submission

February 2025

AISA

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

This submission has been prepared by AISA on the Cyber Security Legislative Reforms Consultation for the Rules and implementation of these legislative changes. AISA has prepared this response using inputs from our membership and senior executive members of our Executive Advisory Board for Cyber (EABC).

We continue to appreciate the engagement provided by the Department of Home Affairs and the Cyber Security Ministers Office. The Cyber Security Reforms Packages have been a large effort between Government, Industry and Practitioners which has resulted in reforms that uplift and mature Cyber Security capability for all Australian Citizens.

We look forward to continued engagement with the Government on its continued 2030 Cyber Security Strategy and its implementation, as we strive to make Australia a safer and more secure nation.

AISA continues to believe that the reforms that relate to Security Standards for Smart Devices has the ability to significantly impact the immediate and future security posture for Australia, it's citizens and businesses.

Cyber Security (Security Standards for Smart Devices) Rules

AISA continues to believe that the reforms that relate to Security Standards for Smart Devices has the ability to significantly impact the immediate and future security posture for Australia, it's citizens and businesses. We agree with the assertion that the previous voluntary measures in 2020 have not been sufficient and does not provide a comprehensive approach.

The proposed reforms that define the responsible entities, standards to be adopted, smart devices to be regulated, introduction timelines and monitoring and enforcement mechanisms are all in line with the consultation and aligned with our views as part of our previous submissions.

We also welcome the pragmatic approach to apply the baseline security standards to Consumer Energy Resources as part of this reform. It is well understood that there is a larger review of Consumer and Distributed Energy Resources, but this ensures that consumers in particular, have some immediate security measures applied and that they are applied more consistently.

We foresee that this specific area of reform will need to continue to evolve and whilst the immediate reforms will significantly uplift security posture for smart devices, we will continue to advocate for continued security uplift in this space.

Cyber Security (Ransomware Reporting) Rules

In regard to the Ransomware Reporting rules, AISA is in agreement with the proposed rules and that they are aligned with our views expressed throughout the consultation period.

Whilst not related to the legislation or rules being proposed, we continue to advocate for a mechanism that enables voluntary reporting for the 93.44% of registered businesses not captured by the legislation and the $3m threshold. These businesses whilst not as impactful to national security bear the burden of Ransomware attacks. This would enable affected businesses to provide detailed

information that is not currently captured by other notification mechanisms, in particular the Notifiable Data Breach reporting. This information could be used to further inform policy, provide support to these entities and uplift security capability across a larger cross-section of Australian businesses.

We also note the inclusion of the Reasonable search or inquiry provision as part of the reforms, this is welcomed as it addresses concerns that affected businesses could find themselves unable to meaningfully report inside of the prescribed timelines. This provision enables the timely reporting of incidents with the information to hand and then the ability to provide further information as it comes to hand.

We continue to advocate for a mechanism that enables voluntary reporting for the 93.44% of registered businesses not captured by the legislation and the $3m threshold.

Cyber Security (Cyber Incident Review Board) Rules

Overall, AISA believes that the proposed Cyber Incident Review Board rules are in line with the consultation process and intentions of the reforms. We remain of the view that the purposed of the Cyber Incident Review Board is to ensure that the public is well apprised of the cause and any recommendations of a significant incident that impacts Australian citizens. These recommendations should ensure that the public and the entities that deliver services to the public can protect themselves and reduce the chance of further similar incidents occurring.

AISA notes that the definition of the types of incidents that would trigger a Cyber Incident Review Board referral is well defined and scoped to incidents that are of concern to the Australian community.

We also note that due consideration has been provided for managing of Conflicts and paid work, which was a significant concern in our initial consultation processes with our Members and Executive Members.

Security of Critical Infrastructure Rules

AISA also welcomes the improvements and streamlining of Critical Infrastructure legislation, in particular the alignment of Telecommunications obligations to reduce complexity and crossover of obligations. The proposed rules align with the consultation, and we support this important reform.

Authored by
Michael Burchell
Chair - AISA Board of Directors
michael.burchell@aisa.org.au

Megan Spielvogel
General Manager, AISA
megan.spielvogel@aisa.org.au