INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

10 February 2026

To the Department of Home Affairs

By submission: Department of Home Affairs Feedback Form

RE: Proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules – Consultation Paper

The Internet Association of Australia Ltd (**IAA**) thanks the Department of Home Affairs (**Department**) for the opportunity to respond to the consultation on the Critical Infrastructure Risk Management Program Rules (**CIRMP Rules**) Consultation Paper and the associated the proposed amendments.

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized Internet service providers (**ISPs**), on whose behalf IAA has been actively engaged in the development of the Security of Critical Infrastructure (**SOCI**) legislative framework as it applies for the telecommunications sector.

From the outset, we recognise and appreciate the ongoing work of the Department to enhance the CIRMP in response to the evolving threat landscape to ensure the appropriate security and resilience maturity of Australia's critical infrastructure. We furthermore appreciate the Department's ongoing commitment to consult with industry and other stakeholders to ensure further reforms to the SOCI framework are fit-for-purpose, proportionate and practicable. We therefore make this submission to support and help ensure that the enhanced CIRMP Rules are appropriate to industry and the community.

We understand that at this stage, the proposed amendments to the CIRMP only intend to capture domain name systems (**DNS**) infrastructure within the communications sector. However, we also anticipate that these enhancements will likely be extended to the telecommunications sector in the future. Furthermore, given the DNS is a fundamental component of the Internet, IAA and our members are interested in the proposed enhancements, which may have direct and indirect implications for ISPs. In addition, IAA's membership also consists of entities operating within the DNS sector.

We therefore offer this response from the perspective of our members, as well as for the public good of the Internet, as an open and public infrastructure. In particular, we note that the DNS is a globally shared coordination system where public disclosure of DNS incidents, misconfigurations and outages is critical to the stability and security of the Internet. We strongly recommend that the proposed enhancements do not unnecessarily constrain DNS operators' ability to make technical disclosures that would weaken the collective situational awareness across the Internet industry.

We limit the scope of our response to the above matters at this stage and welcome the opportunity to engage with the Department and stakeholders further as the draft legislation is developed, and in the event that the proposed enhancements are expanded to the telecommunications sector.

All-hazard 1: Consideration of specified risk advice and Cyber 4: Enhancing cyber material risks

We are concerned that the specified risk advice and enhanced cyber material risk mechanisms, without explicit guardrails, may unnecessarily increase the sensitivity of incident information due to its potential relevance to specified risk advice and result in the weakening of the collective situational awareness that contribute to the resilience of the global Internet.

Under the proposed all-hazard measure 1, DNS operators may be required to assess whether an incident is connected, whether directly or indirectly, to a risk identified in a specified risk advice. Similarly, under cyber measure 4, DNS operators will have to consider specified cyber risks identified by the Government.

We are concerned that this would result in incident information being automatically classified as sensitive, and likely 'protected information' under the *Security of Critical Infrastructure Act 2018* (**SOCI Act**). Due to the prohibitions on using and disclosing protected information, this may cause DNS operators to adopt a defensive and overly sensitive posture, resulting in reduced transparency for the rest of the industry.

We understand there may be legitimate cases where incident information cannot and should not be publicly disclosed for national security and intelligence purposes. However, we are concerned that the confusion over what information can be legally disclosed and fear of regulatory action will result in a trend towards confidentiality.

Furthermore, even in cases where specified risk advice is relevant to an incident, where there is no ongoing security risk, or the disclosure of specified risk advice would improve resilience across the sector, there is great value in DNS operators being able to share incident information with the internet community. Transparency is an established and important practice within the DNS ecosystem that contributes to the improved resilience of the Internet.

Thus, we recommend that the measures are not drafted in a manner that discourages technical disclosure practices. The explanatory statement should explicitly set out that the measure is not intended to constrain DNS operators to making technical disclosures only to government. We also strongly recommend clarification as to the applicability of confidentiality obligations in relation to 'protected information', and specifically, incident information that is connected to specified risk advice or identified cyber and information material risks. We consider guidance material that explicitly sets out when a DNS operator would be expected to keep incident information confidential, and where disclosure to the DNS and Internet community would be considered necessary to mitigate the risk to the availability, integrity, reliability or security of the critical infrastructure asset (and other critical infrastructure assets) under section 42AA of the SOCI Act.

All-hazard 2: Foreign ownership, control and influence (FOCI) Supply Chain 1: supply chain vulnerability mapping and Supply Chain 2: vendors of concern

Similarly, we are concerned that public disclosure of technical faults that relate to offshore vendor errors may be construed as unmanaged FOCI risk and exposure. We note that the DNS infrastructure is inherently global, and FOCI risk is a key concern for DNS operators in their risk management practices. The expectation to consider, minimise and eliminate all material risks associated with FOCI or vendors of concern may again cause DNS operators to err on the side of caution when producing incident reports and result in underreporting out of fear for regulatory action.

We therefore recommend that public reporting of DNS incidents, including where they involve offshore vendors or components is recognised as part of good governance. Supply chain vulnerability mapping should also coexist with transparent disclosure of supply chain related incidents, and should not discourage information sharing that would support industry-wide awareness. Importantly, security incidents related to FOCI risk or vendors or concern, and transparent reporting to the industry in relation to such incidents should not be automatically treated as an admission of failure to comply with the enhanced measures.

We also recommend that the Government's enforcement approach to the enhanced CIRMP measures will be educative and consultative, and as it relates to FOCI exposure and the supply chain, the government explicitly recognises the global and complex nature of the DNS ecosystem, and thus inevitable FOCI and supply chain risks which may not be able to be fully mitigated or eliminated.

Pace of Legislative Reform

We also raise our concerns that the proposed enhancements to the CIRMP Rules are being considered and developed prior to the completion of the Independent Review of the Security of Critical Infrastructure Act 2018 (**Independent Review**). We understand the Independent Review is expected to be completed and reported on in early 2026, and there may be some time for the Department to consider the findings of the Independent Review prior to the finalisation of the legislative drafting of the enhancements to the CIRMP Rules. However, with legislative drafting of the proposed enhanced CIRMP Rules likely to be progressing concurrently, we are concerned that the compressed timeframe will mean the Independent Review Report will not be afforded sufficient consideration and its findings will have limited practical influence on reforms that are already well advanced.

We acknowledge the urgency in ensuring Australia's critical infrastructure legislation keeps pace with technological, social, and threat developments. However, without the outcomes of the Independent Review informing further regulatory work from the outset, there is a significant risk that the proposed obligations will be difficult to amend or revised, even where evidence emerges that adjustments are warranted.

We therefore recommend that at a minimum, the Department defers the completion of the initial legislative drafting and the consultation on the exposure draft until the Independent Review Report is released so that stakeholders are consulted on a draft that reflects the findings of the Independent Review.

Once again, IAA appreciates the opportunity to contribute to the proposed enhancements to the CIRMP Rules. We reiterate our support for a fit-for-purpose regulatory framework that supports entities within the critical infrastructure landscape to meaningfully engage in best practices that will materially result in security and resilience uplifts that improve the overall security posture of Australia. To that end, we offer this submission to help ensure that the enhancements will not curtail established best practices within the DNS and wider Internet community, and that reforms to the CIRMP Rules are informed by the comprehensive review of the SOCI Act.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia Ltd (**IAA**) is a not-for-profit member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IAA regularly engages with government and regulatory bodies on policy matters affecting the Internet industry. In particular, our advocacy efforts represent the small to medium sized internet service providers in Australia who are often disproportionately disadvantaged by law reform affecting the telecommunications sector. Our advocacy work is guided by the following principles:

We stand for an internet for the common good

We stand for an open internet platform

We stand for measured, effective and practical regulation

IAA is also a licenced telecommunications carrier and provides the IX-Australia service to Corporate and Affiliate members on a not-for-profit basis. It is the longest running carrier neutral Internet Exchange in Australia. Spanning seven states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.