Department of Home Affairs
via email ci.reforms@homeaffairs.gov.au

17 November 2022

To whom it may concern,

Submission: Consultation on the proposed Risk Management Program (RMP) as part of Australia's critical infrastructure reforms

On behalf of PwC Australia (PwC), I am pleased to make this submission (Attachment 1) to the Department of Home Affairs' consultation on the proposed RMP, a key supporting component of Australia's critical infrastructure reforms. These reforms are essential to help secure Australian critical infrastructure assets, taking a holistic approach to security that encompasses cyber, physical, personnel and supply chain security.

PwC is supportive of the Federal Government's commitment to securing Australia's critical infrastructure and the finalisation of RMP rules is a key step of the journey, providing captured entities with greater clarity in relation to their reporting obligations. Our team is working closely with clients to help ensure they are meeting their obligations under the critical infrastructure reforms and, above all else, they seek certainty, particularly in relation to RMP reporting. This will help them plan for now, for the future and help provide them with a roadmap for continual improvement. It will also help secure Australian critical infrastructure assets more effectively and rapidly.

I note the RMP rules have a focus on reducing reporting duplication across divergent regimes, which is commendable. And by considering the unique circumstances of all captured entities - not taking a 'one-size-fits-all' approach - the reforms will reduce regulatory burden on those entities with limited resources. Furthermore, by limiting RMP reporting to 13 asset classes, the Cyber and Infrastructure Security Centre (CISC), which will regulate the regime for 12 of these asset classes, will be able to have greater oversight of those assets which are most critical to the security of the nation.

While we support the intent and implementation of the RMP, there are several key areas, as explored in this submission, where we believe amendment or greater clarity is required.

These include:

- varying implementation periods across security domains
- the need for RMP templating guidelines
- clearer guidance as to the level of detail to be included in RMPs
- interdependency analysis
- information sharing

I thank you for considering this submission. If you have any queries or would like to discuss any issues raised further, please do not hesitate to contact me on

Yours faithfully,

Robert Di Pietro
PwC Australia Partner
Cybersecurity & Digital Trust Lead

Attachment 1: Consultation response

Varying implementation periods across security domains

We note the proposed grace periods for captured entities to meet their RMP reporting obligations are:

- six months from the rules being finalised to develop their written program
- an additional 12 months to comply with one of the cyber frameworks outlined in the rules (or equivalent)

In practice, this means that for cyber requirements of the RMP to be enacted, there will be a timeframe of 18 months before they must be implemented. In the face of ever-increasing and evolving cyber threats, the provision of 18 months for framework compliance is significant.

While PwC does not disagree with the need for an 18 month phase-in for cyber compliance, we submit that the proposed framework should be articulated in the initial RMP reporting (six months), with a clear roadmap to compliance at 18 months. This will, in effect, help ensure that captured entities are planning with the end in mind, rather than deferring cyber uplift longer than necessary. This is also important given the considerable amount of time cyber uplift and compliance with a framework can take.

The need for RMP templating guidelines

We note there is no standard templating set out for RMPs, meaning organisations must develop their own reporting format. While we note the reasoning behind the lack of standard templating, as highlighted in the guidance,[1] we submit that at least in the early stages of RMP reporting, the development of an optional standard template would be advisable. This would provide clear guidance for captured entities to help ensure they fulfil their reporting obligations and, across sectors, assist in the development of key sector-specific metrics and indicators that can be compared over time. Furthermore, considering the issue of optional standardised templating from the CISC's perspective, it may assist in attaining consistent reporting of risks, trends, issues and themes, as well as removing additional administrative burden that could occur if organisations were left to their own devices. If addition of an optional standardised template was considered, technology could be leveraged to create an online submission tool for ease of reporting and analysis by the CISC.

[1] https://www.homeaffairs.gov.au/reports-and-pubs/files/draft-risk-management-program-guidance.pdf, P16

Clearer guidance as to the level of detail to be included in RMPs

As noted in the guidance, "the level of detail in a risk management program is determined by the individual entity, and will require the approval of your board, council or other governing body if you have one".[2] While it is favourable that over time organisations develop greater autonomy in ensuring the detail included in RMPs is appropriate, there is a case for the provision of clearer guidance during early implementation. To this end, we submit that during the formative period of reporting that the level of detail included should be commensurate with the severity of the risks and the information available, setting a benchmark for comparison over time and, for the CISC, helping provide a clearer picture of the maturity of entities across diverse sectors. This will also assist in providing boards, councils and other governing bodies with the correct amount of detail they require to confidently provide RMP attestation.

Interdependency

The guidance asks for entities to provide a view of interdependency of critical infrastructure within their organisation and on other critical infrastructure externally (paragraphs (d) - (i) of subsection 5(2) of the RMP Rules). Mapping of these interdependencies internally and externally is an effective risk management process and provides companies with a better view of single points of dependency and failure. We submit, however, that further clarity as to how to conduct this type of assessment and, in turn, report it, is required. This would benefit both government and industry, supporting nation-wide mapping of key dependencies. Utilisation of an assessment or survey approach would support such mapping, facilitating a more rapid and accurate assessment for the entity and for government, as it would identify key areas of reliance.

Information sharing

The government has collected - and will continue to collect - a wealth of information about the vulnerabilities and dependencies of Australian industry. There is a clear opportunity to better leverage the trusted information sharing networks (TISNs) to uplift information sharing, both sectorally and cross-sectorally, to support a continuous cycle of collection, analysis and information-sharing contribution nationally. Over time, this may also serve to identify trends in the threat and vulnerability landscape. Achieving local situational awareness will be beneficial to Australian industry, as will the long-term resilience that participation of large multinational corporations operating in a global context can contribute.

[2] https://www.homeaffairs.gov.au/reports-and-pubs/files/draft-risk-management-program-guidance.pdf, P16