Please see below the Qualtrics Response to the *References:*

A. *Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*

B. *Explanatory Statement – Security of Critical Infrastructure (Application) Rules 2021*

C. *Protecting Critical Infrastructure and Systems of National Significance – Industry Town Hall, 25 Nov 21*

D. *Policy 8 Sensitive and Classified Information, Australian Government Protective Security Policy Framework*

To whom it may concern

On behalf of Qualtrics, we greatly appreciate the ongoing opportunity to participate in security-of-critical-infrastructure reforms. Qualtrics has been liaising with SAP, our parent company, and SAP Australia, its local affiliate, who has been actively engaging with and has had significant involvement in co-design activities, including the risk management program (RMP) rules, and discussions relating to the proposed definition changes between the 2021 and 2022 bills associated with the Data Storage or Processing Sector.

Risk Management Program

SAP and Qualtrics have one remaining question that remains outstanding regarding RMP timelines, and we jointly offer a suggestion that we believe will contribute to industry's capacity to successfully implement the RMP, a key feature of Reference A.

As the supporting rules for the 2022 bill are developed, will there be a grace period for the RMP obligations, as has been noted in Reference B for the registration of critical infrastructure assets and for cyber security incident reporting and response?

If not under consideration, we suggest a grace period of six months.

We note that the RMP rules, as currently drafted and presented in Reference C, state for each of the requirements (other than the standards and frameworks requirement) that "… responsible entities must, within six months of the commencement of this rule, ensure that their risk management program …[action]". From SAP's experience being a critical infrastructure asset owner in Germany, the grace period to become fully compliant was 24 months, a time frame that was fitting the scale of the internal project to achieve compliance.

A grace period of six months would add an additional six months to the various requirements in the draft RMP rule, affording industry 12 months from the commencement of the rule to effectively plan and implement alignment of risk-management practices with the legislation, and any necessary capability uplift. While not 24 months per SAP's experience in Germany, we believe 12 months is appropriate for the risk-based approach being undertaken. 12 months would push the standards and frameworks requirement out from 18 to 24 months, a timeframe that is consistent with SAP's German program, which strongly features standards/frameworks compliance and audit.

We contend the additional time would support the achievement of optimal risk management and associated security outcomes, increasing the CI providers' capacity to support the intent of the legislation. The additional time would also be beneficial for gaining all necessary internal approvals, noting that the legislation places an onus on the Responsible Entity, which will in most scenarios, in the case of a multinational company, be the CEO and Executive Board.

Asset definition

Regarding the definition changes presented in the 2022 bill, we commend the improvements. However, we wish to reiterate a suggestion previously communicated in and around the asset definition workshop of 15 November.

We note that the inclusion of a 'business critical' data threshold to identify critical data storage or processing assets based on the consumption of Australian-based cloud services by critical asset owners across critical sectors is an excellent mechanism to ensure a risk-based approach to regulation. It seeks to guard that only those cloud services that, if rendered unavailable, would pose an unreasonable risk to the delivery of essential services, are subject to the positive security obligations. We feel; however, that the lack of a 'business critical' data threshold relating to the consumption of cloud services by government agencies and body corporates will lead to identification of cloud services as critical assets, which if unavailable, do not pose a level of risk to Australian society, the economy and national security that warrants critical status and associated costs.

Therefore, we suggest the inclusion of a 'business critical' data threshold for Federal, State and Territory government agencies and body corporates to identify if a cloud service poses justifiable risk to require registration as a critical asset. We propose that the Business Impact Levels tool at Table 1 in Reference D as a ready-made and simple assessment process for government agencies and body corporates to use. We offer that Business Impact Level 2 in Table 1 is an ideal business critical data threshold because it allows agencies and body corporates to consider the range of impacts that the compromise of the data stored or processed in/by the cloud service could present.

Noting that Reference D is subject to policy change over time, we suggest alignment to it for the purposes of a 'business critical' data threshold for government agencies and body corporates could be through a Rule to the Act rather than codified into the 2022 bill.

We note that critical asset owners are obligated to advise a service provider that a 'business critical' data threshold requiring asset registration has been met. We understand that government agencies and body corporates are not critical asset owners; thus, this obligation does not currently apply. Therefore, we suggest that onus be placed upon the cloud asset owner to confirm with its government agency or body corporate customer whether the 'business critical' data threshold applies.

Thank you for the opportunity to provide our feedback to the legislation. Qualtrics welcomes the opportunity to continue to have constructive dialogue in relation to the development of the regulatory framework governing critical infrastructure.