



1 February 2022

Department of Home Affairs
Commonwealth of Australia

(Submission lodged via email)

RE: Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Amazon Web Services (**AWS**) welcomes the opportunity to make a submission on the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (the **Bill**). We continue to support the Australian Government's objective of enhancing the security and resilience of Australia's critical infrastructure.

Sector and asset definitions

AWS welcomes the amended definition of a data storage or processing service at a sector level. However, we maintain our view that an objective standard is necessary for the identification and declaration of national critical infrastructure assets for our sector. This approach will ensure the fair and consistent application of all obligations, and will provide critical infrastructure entities with regulatory certainty.

Risk Management Program

AWS supports the introduction of sector-neutral, principles-based Rules relating to the Program. The development of these Rules has been the result of extensive consultations across all sectors, and we thank the Department for working closely with industry to create a practical framework across such a broad section of the Australian economy. In particular, we welcome the recognition of strategic certification under the Hosting Certification Framework (**HCF**) as meeting the requirements of the Program. This is a pragmatic step that avoids regulatory duplication and sets an appropriately high bar for security risk management in the data storage or processing sector.

To ensure regulatory certainty in relation to the Program, we ask that:

- **The minimum time periods for compliance set within the Rules (i.e. six months from being 'switched on') be specified in legislation;**
- **The consultation period for new Rules be extended from 28 days to 42**, in recognition of the likely technical complexities to be considered within and across sectors;
- **Clarification be provided as to whether the annual reporting requirement for the Program is met by ongoing certification under HCF.**

Systems of National Significance

In principle, AWS agrees with the approach of a tiered system of critical infrastructure asset classification. However, the process by which these declarations are made does not adequately consider the likely regulatory impact on owners and operators of a SoNS. The Bill provides the Minister for Home Affairs (the **Minister**) with broad discretionary powers to declare a small subset of critical infrastructure assets as SoNS, following a short period of consultation with impacted entities. These SoNS are to be the most sensitive for Australia's national cyber resilience, particularly when interdependencies between critical



infrastructure assets and sectors are considered. The Bill also allows the Minister to make a declaration without an equal expectation that the owner or operator of the designated asset is provided enough time or information to prepare an informed response.

To address this, we recommend:

- **The 28-day consultation period be extended to 42 days** given the complex, highly technical and specialised nature of the assets likely to be considered for declaration as a SoNS. In that vein, we recommend that the provision allowing the Minister to set a shorter timeframe than 28 days in ‘urgent circumstances’ be removed. It is unclear what circumstances would necessitate forgoing appropriate consultations, especially given the potentially intrusive nature of the applicable enhanced cyber security obligations. We also urge the inclusion of a provision in the Bill that requires the Minister to demonstrate having shown regard for submissions made by an impacted entity in response to a declaration notice.
- **The Minister should be required to share the rationale for the declaration of a SoNS with the impacted entity.** The Bill allows for the Minister to withhold this information on the grounds of it being prejudicial to security; however, given these declarations will likely all be made on national security grounds, this creates an extraordinary lack of transparency for impacted entities. The absence of this information will prohibit the entity from making a fully informed submission to the Minister regarding the declaration, and may even hinder the ability of the entity to appropriately manage its cyber security risks by withholding important information on threats to the entity’s own assets.
- While we agree that the declaration of a SoNS should be considered protected information, we believe this provision should be amended to **allow entities to disclose the declaration when necessary to meet its obligations under the Program or in carrying out directives under the enhanced cyber security obligations.** This should extend to trusted third parties and partners, or other critical infrastructure customers or service providers.

Enhanced cyber security obligations

The enhanced cyber security obligations are an important and potentially intrusive set of obligations with a significant regulatory impost. As these obligations would apply to the most sensitive assets meeting a high threshold for interdependencies and national significance, we believe there should be an equally high threshold for their enforcement. We recommend:

- **Amending the Bill to extend the Secretary’s requirement to consult with entities to 42 days.** In making a final decision, the Secretary should be required to demonstrate having shown regard for any submissions made by the impacted entity.
- **The Bill should define specific criteria the Secretary must have met before enacting any of the enhanced obligations.** Specifically, the Bill should recognise that disagreement with an entity on the necessity or technical feasibility of a direction are not reasonable grounds for the appointment of a designated officer or a mandate to install software. Even when the Secretary does consult, the Bill allows them to make the final decision based on their subjective view and irrespective of whether the entity agrees. This is particularly true of the requirements for vulnerability assessments or providing system information, where the Secretary may subjectively decide whether they believe the entity has the technical ability or capacity to comply with a direction.



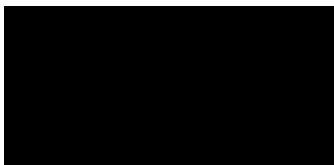
- **Amend the Bill to ensure that entities can benefit from full immunities and indemnities when complying with an Enhanced Cyber Security Obligation.** The Bill does not provide an entity with any immunities when complying with an enhanced obligation. For example, when the entity has to comply with a cyber security exercise, vulnerability assessment, or information access request and such compliance may require an entity to provide confidential information of a third party (which may or may not be in contravention of a non-disclosure agreement between the entity and that third party). This is not a reasonable position to be placed in. The Bill should grant immunity to an entity when it is complying with an enhance obligation and include an indemnity for any third party claims that are caused by compliance with such obligations.
- **Amend the Bill to ensure that entities may recover their reasonable and actual costs of compliance with an enhanced cyber security obligation.** Entities cannot recover the actual costs of compliance with Government directions and may be left out of pocket. This is an unacceptable position for an entity to accept given compliance with a Government direction, in situations under the threat of civil penalty or imprisonment, may have a material or significant impact on an entity's business, operations, or customers or require significant resources and cost. The Bill should allow an entity to recover the reasonable and actual costs of compliance with a Government direction.


Independent authorisations and oversight

Throughout the consultation process, AWS has maintained that independent, statutory authorisation and oversight is necessary and appropriate for the transparent, proportionate, and proper functioning of the critical infrastructure reforms. We continue to hold this view. AWS agrees with the Parliamentary Joint Committee for Intelligence and Security (**PJCIS**) recommendations for more robust authorisation and oversight processes, and we strongly support the recommendation for a technical support body (Recommendation 6). However, we consider it appropriate for this body to exist as an independent statutory office holder. The Cyber and Infrastructure Security Centre, as the regulatory entity sitting within the Department, lacks this necessary independence.

We look forward to partnering closely with the Department on the ongoing development and implementation of these important reforms.

Best regards,



Roger Somerville (**)**
Head of Public Policy, Australia and New Zealand
Amazon Web Services.