The Hon Tony Burke MP
Minister for Home Affairs,
Minister for Immigration and Multicultural Affairs,
Minister for Cyber Security,
Minister for the Arts, and
Leader of the House of Representatives

14 February 2025

Dear Minister

Thank you for the opportunity to provide comments on the Subordinate Legislation (Rules) for the 2024 **Cyber Security Legislative Package.** The comments below address matters concerning the following Rules:

- Cyber Security (Security Standards for Smart Devices) Rules 2024
- Cyber Security (Ransomware Payment Reporting) Rules 2024
- Security of Critical Infrastructure (Critical infrastructure risk management program) Amendment (Data Storage Systems) Rules 2024 (Data Storage Systems Rules)

Cyber Security (Security Standards for Smart Devices) Rules 2024

The Government's alignment with the United Kingdom's *Product Security and Telecommunications Infrastructure Act 2022* (UK PSTI Act), and its associated regulatory regime, is welcomed. Harmonisation with the UK PSTI Act will reduce regulatory complexity and uncertainty for manufacturers. As compliance obligations will come into force 12 months after the Rules take effect, manufacturers of relevant smart devices should have sufficient time to ensure their products meet the requirements outlined in the Rules.

While a 12-month phase in of the compliance obligations for manufacturers is an appropriate practical measure, the commercial circumstances of suppliers and retailers necessitates an additional measure. A phased approach for suppliers'/retailers' compliance obligations that provides a further 12 months to comply after the manufacturers' compliance date would align with the practical realities of global supply chains. Without a staggered approach, suppliers/retailers may find themselves in the position of holding non-compliant devices that were manufactured and acquired before the compliance obligations began. This could lead to significant financial losses, operational disruptions and potential e-waste. If compliance commences simultaneously across the supply chain, a situation could arise where suppliers/retailers hold non-compliant devices, but manufacturers would not be liable as the devices were produced before their compliance obligations began.

A phased approach would provide a practical transition period for suppliers/retailers to manage their existing inventory and align their stock with the new compliance requirements. This approach would allow for a more orderly and non-disruptive transition to the new regulatory regime across the entire supply chain.

Cyber Security (Ransomware Payment Reporting) Rules 2024

We support the proposed Rules but note that there continues to be no proposed 'safe harbour' for entities in relation to potential criminal liability, particularly under Commonwealth laws, in respect of information disclosed through Ransomware Reports. We recognise this is a matter that involves competing policy objectives. Organisations and individuals would benefit from guidance and/or a legislative amendment that clarifies their obligations and clearly expresses the Commonwealth's expectations.

Security of Critical Infrastructure (Critical infrastructure risk management program) Amendment (Data Storage Systems) Rules 2024

In our submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Inquiry into the Cyber Security Legislative Package in October 2024, Amazon Web Services (AWS) drew the Committee's attention to the importance of the Act (and the Rules) clearly allocating responsibility as between critical infrastructure asset owners and operators for the operation and protection of data storage systems that are part of a critical infrastructure asset. In our submission we gave an example of a responsible entity, 'Bank', that operates a critical banking asset and also operates a data storage system holding business critical data in connection with the critical banking asset (e.g., a database containing personal information of Bank's customers). Should 'Bank' choose to host the data storage system on a critical data storage or processing asset operated by another responsible entity, the data storage system should be considered part of the critical banking asset and the responsible entity 'Bank' should be responsible for the operation and protection of the system.

As a cloud services provider (CSP), AWS is aware of the complexity and many varieties, of data storage systems that owners and operators of critical infrastructure assets might deploy and use. The allocation of responsibility for the operation and protection of those data storage systems needs to be clearly and definitively understood by all parties.

AWS appreciates the efforts of the Department of Home Affairs ('the Department') to provide clarity through the Rules and via guidance. It is our strong view that both private and public sector critical infrastructure asset owners and users would benefit from further Departmental guidance that addresses specific examples of data storage systems that are part of a critical infrastructure asset. AWS supports this guidance being provided in the form of Guidance Notes, Fact Sheets, or similar collateral issued by the Department. AWS welcomes the Department's release of a Fact Sheet on Schedule 1 – Data storage systems that hold business critical data - and would be pleased to support the Department in the development of further guidance that demonstrates by example the application of the Rule, particularly as it may pertain to services offered by CSPs.

In our PJCIS submission last October, we also noted that the proposed amended definition of protected information, under Section 5A, appropriately expanded the concept of protected information to cover documents and information that should be protected by the SOCI Act. Given that protected information may include information that has the potential to compromise the operation of a critical infrastructure asset, as well as other highly sensitive commercial information, we submitted that government authorities and representatives who receive protected information should be required to handle that information at least at a level commensurate with the Commonwealth's data classification of SECRET, as per the Protective Security Policy Framework (PSPF) Policy 8: Classification System v2018.8.

We would welcome a proactive approach by the Department, at the earliest possible opportunity, to explicitly clarify requirements for appropriate security classification of protected information obtained under the SOCI Act by government employees and contractors. We would further support the express requirement that the handling of all protected information be conducted with reference to an explicit data lifecycle mandate that confirms timelines for deletion of all protected information.

As ever, AWS is ready and would be pleased to provide further material in support of the positions set out above and to assist officers of the Department as required.

Yours sincerely

Roger Somerville
Head of Public Policy, Australia and New Zealand
Amazon Web Services