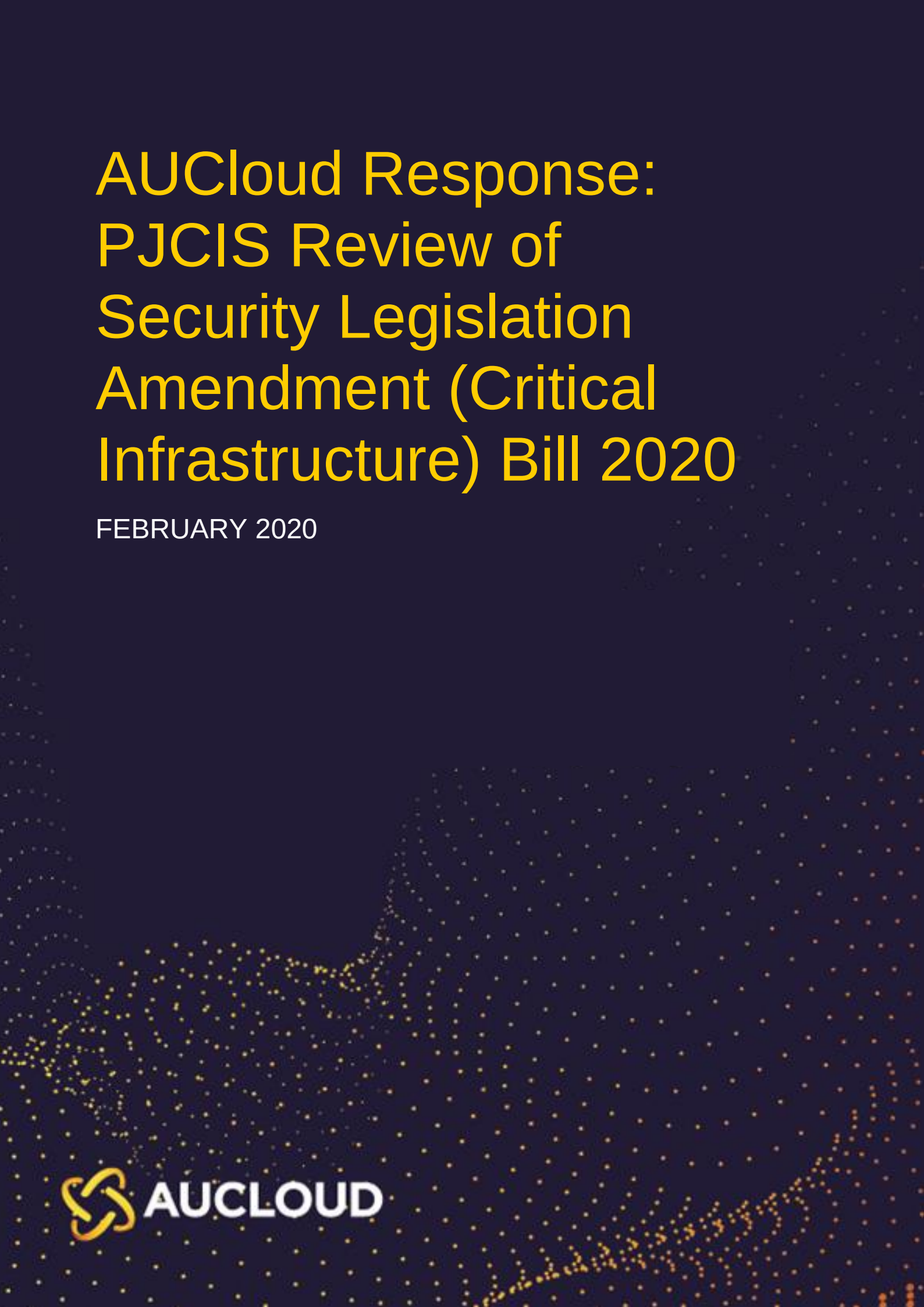
AUCloud Response: PJCIS Review of Security Legislation Amendment (Critical Infrastructure) Bill 2020

FEBRUARY 2020



Disclaimer

The information in this Proposal is the confidential information of Sovereign Cloud Australia Pty Ltd ("AUCloud"). Such information must confidential at all times and used solely to consider the Proposal put forth by AUCloud. You agree to take such measures to prevent the disclosure of the information as you would to prevent the disclosure of your own proprietary information, but in all cases, shall use at least reasonable care.

You do not acquire any rights in the information. All AUCloud trademarks and logos belong to Sovereign Cloud Australia Pty Ltd. Other trademarks and logos belong to their respective owners and are used for informational purposes only.

The contents of this document constitute valuable proprietary and confidential property of AUCloud and are provided subject to specific obligations of confidentiality set forth in one or more binding legal agreements. Any use of this material is limited strictly to the uses specifically authorised in the applicable license agreement(s) pursuant to which such material has been furnished. In the event there are no applicable license agreement(s) governing the use of this material, please be advised that any use, dissemination, distribution, copying or disclosure of all or any part of this material not specifically authorised in writing by AUCloud in advance is strictly prohibited.

This is not a legally binding document and is submitted for information purposes only. Due to the forward-looking nature of this document, AUCloud's response may include information about solutions or products that may be in the planning stage of development or that may represent custom features or product enhancements. Feature and functionality cited in this document that is not publicly available or generally available today is discussed within the context of the strategic evolution of the proposed products. AUCloud is under no obligation to provide such future functionality.

Table of Contents

Introduction

AUCloud welcomes the opportunity to lodge this submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) as part of their review into the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and a Statutory Review of the Security of Critical Infrastructure Act 2018.

AUCloud is a sovereign cloud Infrastructure-as-a-Service (IaaS) provider, exclusively focused on meeting the data and security related needs of the Australian Government and Critical National Industry (CNI) communities. In December 2020 AUCloud listed, with confidence, on the Australian Stock Exchange.

As an Australian owned and operated cloud provider our number one priority is securing the data of Australians, in Australia. Our business is premised on ensuring the highest level of cyber security with security by design features engineered into our platform from the ground up. With the current focus on ensuring Australia's national security, we strongly endorse the Review of this legislation, having regard to the adequacy of the legislation in addressing the national security threats and risks posed to the Australian economy.

AUCloud fully endorses the objectives of the *Security of Critical Infrastructure (SOCI) Act* and recently also contributed to the Department of Home Affairs invitation to review the Exposure Draft of proposed amendments to the Act.

This response provides comments related to the updated Legislation under review by the Committee. We would be happy to present before the Committee if required.

About AUCloud

With security core to how we operate, AUCloud was the first cloud provider to achieve IRAP status to the PROTECTED controls of the Australian Cyber Security Centre's (ACSC) Cloud Assessment and Authorisation Framework (CAAF). This applies across our two independent environments: our Official Data Community Environment (ODCE) and our PROTECTED Data Community Environment (PDCE) that meet or exceed these controls.

In addition, AUCloud's IaaS offerings and supporting business processes are certified against the International Standard for Information Security (ISO/IEC 27001).

As a sovereign IaaS provider, AUCloud is owned, managed and operated in Australia. All services and data managed by AUCloud remain in Australia ALWAYS (including metadata, monitoring data and derived analytics data). All AUCloud services are monitored and operated in Australia by Australian citizens who have been security cleared to Australian Government standards.

AUCloud operates from two Data Centres: Sovereignty Zone 1 in Canberra and Sovereignty Zone 2 in Sydney, both designed to meet ASIO T4 standards for Zone 4 security.

AUCloud solutions enable customers to benefit from sovereign data protection with the scale, automation, elasticity and lower costs typically associated with global cloud offerings. The specific services we provide include:

- Back-up as a Service
- M365 Backup as a Service
- Disaster Recovery as a Service
- Storage as a Service
- Compute as a Service
- Virtual Desktop as a Service.

We also support a range of diverse partners, including Software as a Service and Platform as a Service providers in the delivery of services to their customers.

With deep expertise in data storage processing and related services, we believe we are well placed to provide an informed contribution to the Review.

Overview

AUCloud endorses the expansion of Critical Infrastructure Industries defined in the Security Legislation Amendment (Critical Infrastructure) Bill 2020. With deep, practical experience in cyber security, AUCloud appreciates the potential vulnerabilities of operating in a ubiquitously connected, always on, digital environment. We understand the changing nature of how critical infrastructure industries operate in this context and the increasing interconnectedness and interdependence of their operations. We equally understand the security risks posed by cyber vulnerabilities, the impact of cyber disruptions and the corresponding threat to the resilience of Australia's critical Infrastructure and ultimately individuals, communities, business and the Australia's economy.

One of the key learnings of 2020 is the need for greater sovereign resilience. This is NOT about protectionism or isolationism but certainty of sovereign capability and appropriate protection of sovereign assets to support the business of government and livelihood of citizens. Effective risk mitigation to assure protection of critical infrastructure and the ability to rapidly pivot and respond to unforeseen circumstances is imperative.

We therefore endorse the scope and intent of the legislation and welcome the clarification of several issues following the ability to comment on the Exposure Draft of the Legislation in November last year.

Comments

AUCloud identified five specific areas requiring further consideration as part of the review of the Exposure Draft Legislation. In summary these related to:

1. **The definition of 'Data' for the purpose of defining the Data Storage and Processing Sector. The definition was vague and inconsistent with that applied elsewhere by Government.**
2. **The definition of storage and processing as these relate to data. The definition appeared to apply only to physical data centres.**
3. **The recommendation that in relation to the Data Storage and Processing sector, the scope apply only to IaaS with PaaS and PaaS services excluded (on the basis that security controls could be achieved by other means and the complexity of managing the sheer number of PaaS and SaaS providers).**
4. **Consistency of cloud security standards/process across CIs and alignment with policy frameworks applied by government to ensure cross industry security integrity.**
5. **Application of the same standards/process where a Critical Infrastructure sector organisation is operating an on-premise (or self-managed) environment, including where the organisation is migrating to the Cloud.**

While these have largely been met through the tabling of the legislation, for the purposes of Review by the PJCIS we would reiterate the following points for further consideration.

We are satisfied that Point 2 above has been addressed.

1. **In relation to Point 1** (above): For avoidance of doubt and to ensure consistency of definition of data we strongly recommend that the Explanatory Memorandum (EM) elaborate its commentary to clarify: "Data" is defined in a non-exhaustive manner to include information in any form**, *including data types, such as customer data, account data, metadata and support and administrative data***. This consistent with the definition outlined in the Australian Cyber Security Centre's (ACSC) Cloud Assessment and Authorisation Framework (CAAF) which advises:

> *There are a variety of data types used in cloud computing, and cloud consumers need to understand what these data types are, where they exist, and how they are handled and secured. Upon understanding the different data types and how they are managed by a CSP, cloud consumers can then make informed decisions about where to store their information that is appropriate to the data's sensitivity and classification, reducing the risk of it being handled inappropriately.*
>
> *The most common data types in cloud are:*
>
> - ***Customer data:** This is data the cloud consumer creates, generates or uploads to the CSP for storing, processing and sharing using the CSP's cloud services, this includes the cloud consumer's authentication data. The cloud consumer, as the data owner, remains accountable for the security of this data type, including any compromises, losses or damages that occur.*
> - ***Account data:** This is data about the cloud consumer's account with the CSP and can include billing information, contact information and usage information.*
> - ***Metadata:** This includes data about the cloud consumers' use of the CSP's cloud services and can include cloud consumer generated information such as resource names, service tag details and utilisation information.*
> - ***Support and administrator data:** This data type is provided to the CSP's support personnel and administrators for technical support purposes. This can include logs, monitoring alerts and error report information.*
>
> (Anatomy of a Cloud Assessment and Authorisation https://www.cyber.gov.au/acsc/government/cloud-security-guidance)

Alignment of the definition ensures consistency across Government and CI organisations and clarifies that information in any form, also applies to protection of data types such as the metadata, analytics etc that relate to, or are derived from, the information. This is important because if breached, these broader data types also undermine the security, integrity and privacy of systems and data.

2. **In relation to Point 3** (above): The EM clarifies that the data storage and processing services include IaaS and PaaS services and may include SaaS services where *the software is relied on to store or process a Government agency's data or critical infrastructure asset's business critical data as the primary function of the service.*

   There are significant differences in nature between IaaS, PaaS and SaaS services. Given the high number of PaaS and SaaS services in the market, application of the legislation will be complex, difficult to manage and a regulatory overhead for smaller providers. We believe SaaS and PaaS data storage and processing related risks are manageable via other control routes, including through application of the Government's Cloud Assessment and Authorisation Framework (CAAF).

   We believe encouraging application of the CAAF more broadly in relation to the use of cloud services ensures a consistent best practice benchmark across government and critical infrastructure organisations at a data storage and processing level; includes inherent continuous monitoring obligations; and requires

services to advise material changes in the scope or nature of service. It also ensures customers, ie critical infrastructure organisations are making contextual and informed risk-based decisions in accordance with a transparent framework.

3. **In relation to Points 4 and 5** (above): With changes introduced by the ACSC in 2020, IaaS is subject to best practice security assessment and compliance requirements in accordance with the CAAF (see above). The CAAF is underpinned by the IRAP (Information Security Registered Assessors Program) against the controls of the Information Security Manual (ISM) and processes of the Protective Security Policy Framework (PSPF). Noting that these standards are the security benchmark endorsed by Government for its own purpose, we believe the requirements of the CAAF and IRAP align with the intent of the Legislation and consideration should be given to extending this best practice benchmark to other Critical Infrastructure sectors as it relates to data storage and processing.

   The policy provides a clear framework for assessing risk as it relates to the use of cloud services by a specific organisation and requires that organisation to appropriately assess and risk mitigate against known areas of technical, business and operational vulnerability. It does not mandate which services to use but ensures transparent competitive practices and a level playing field in relation to security risk mitigation.

   For consistency this same framework should be recommended to CI organisations operating an on-premise (or self-managed) environment and organisations migrating to the Cloud.

Conclusion

AUCloud believes that the various elements of work currently being progressed by the Government in relation to Australia's cyber security risk mitigation and overall cyber and sovereign resilience should complement each other and are, in fact, strengthened by ensuring this is achieved. We believe it makes perfect sense to build on what Government has already decided is the standard for itself. We would question why Australia would satisfy for anything less in the context of protecting the critical infrastructure that is the backbone of our economy, the foundation of our democracy and the livelihood of our citizens.

AUCloud would be pleased to present before the Committee to clarify our position on these points and in support of strengthening Australia's cyber security posture in support of our critical infrastructure and national data.