# AUCloud Response to Security Legislation Amendment (Critical Infrastructure) Bill 2020

NOVEMBER 2020

AUCLOUD

# 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.

All rights are reserved.

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 is pleased to provide comment on the Draft *Security Legislation Amendment (Critical Infrastructure) Bill 2020* released November 2020.

AUCloud is a sovereign cloud Infrastructure-as-a-Service (IaaS) provider, exclusively focused on meeting the needs of the Australian Government and Critical National Infrastructure (CNI) communities. The scope of the legislation is, therefore, very relevant to the operations and service offerings of AUCloud.

With security core to how we operate at AUCloud, we can advise we are 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.

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

With deep expertise in data storage processing and related services, AUCloud is well placed to provide informed comment on the Draft Legislation.

# Summary

AUCloud understands the intent of Government in reforming the *Security of Critical Infrastructure (SOCI) Act*. 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 Australia's sovereign resilience.

We note a range of recent announcements and/or activities in development by Government also aimed to mitigate cyber related risk with a view to strengthening Australia's resilience. For example:

- Australia's Cyber Security Strategy 2020;
- The Draft Critical Technology Supply Chain Principles;
- The Data Availability and Transparency Bill and Accreditation Framework;
- ACSC's Cloud Assessment and Authorisation Framework ("CAAF").

In support of the common intent and underlying themes of these and the draft *Security Legislation Amendment (Critical Infrastructure) Bill 2020*, AUCloud supports the draft legislation with the following caveats, which will be explained in this response.

1. **The current definition of Data for the purpose of defining the Data Storage and Processing Sector (*Data includes information is any form)* is vague and inconsistent with the definition applied elsewhere by Government.**
2. **The definition of storage and processing, as these relate to data, is not clear and requires definition.**
3. **Acknowledging the criticality of Australia's Critical Infrastructure sectors and the potential impact of disruption or damage, AUCloud agrees that data storage and processing is a 'sector' in itself (as well as the potential underpinning infrastructure for other sectors) and should, in principle, be subject to the proposed legislation. However, we recommend that the scope of the proposed legislative changes for cloud services, apply to IaaS with SaaS and PaaS services excluded.**
4. **With recent changes introduced by the ACSC, IaaS is subject to best practice security assessment and compliance requirements in accordance with the CAAF. 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 largely align with the intent of the draft 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.**
5. **Noting the proposed CAAF benchmark, and to ensure consistent security risk mitigation, where a Critical Infrastructure sector organisation is operating an on-premise (or self-managed) environment, they should also be required to undertake and satisfy an IRAP assessment. Similarly, where a Critical Infrastructure organisation is migrating to the Cloud, those services should be assessed under the CAAF.**

# Detailed Response

1. **The current definition of Data for the purpose of defining the Data Storage and Processing Sector (*Data includes information is any form)* is vague and inconsistent with the definition applied elsewhere by Government.**

   The ACSC's CAAF, released in July this year, provides a clear definition of data, its scope and elements. The CAAF acknowledges there are a variety of data types, the most common including customer data, account data, metadata and support and administrative data.

   AUCloud believes the CAAF definition is equally relevant to other sectors and should be applied to Critical Infrastructure organisations. The definition is specific, can be operationalised and ensures consistency with current Government application of the term in a cyber security context.

2. **The definition of storage and processing as these relate to data is not clear and requires definition. We suggest the following to align with contemporary technology terminology and methods.**

   - Storage: Storage of data in all forms on computer hardware and software systems.
   - Processing: Processing of data in all forms on computer hardware and software systems triggering new processes or creating new data for Government and Critical Infrastructure industry sectors.

3. **Acknowledging the criticality of Australia's Critical Infrastructure sectors and the potential impact of disruption or damage, AUCloud agrees that data storage and processing is a 'sector' in itself (as well as the potential underpinning infrastructure for other sectors) and should, in principle, be subject to the proposed legislation. However, we recommend that the scope of the proposed legislative changes for cloud services, apply to IaaS with SaaS and PaaS services excluded.**

   The Bill does not include a definition of cloud services for the purpose of data storage and processing entities, services etc. However, the Explanatory Memorandum (Paragraph 77) advises that the sector definition (in addition to enterprise data centers, managed service data centers, colocation data centers and cloud data centers) also includes the three types of cloud services: Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS).

   We would make two points. First, the definition of 'cloud data centers' infers that the data storage and processing critical infrastructure asset is a physical asset. Cloud services are hosted on physical and virtual infrastructure in a physical data center but to the extent that services are themselves virtual, are equally at risk of confidentiality, availability, integrity and reliability compromise as per Section 8G of the Draft Bill.

   To ensure the Bill achieves the intent proposed, i.e., appropriate cyber security risk mitigation and management, the scope of Critical Infrastructure Assets should clarify that cloud services are not appropriately defined in terms of cloud data centers. The current 'interpretation' overlooks the responsibility and accountability cloud service providers are expected to have in relation to securing the data of their customers/clients – including underpinning the operations of other (as defined) critical infrastructure sectors.

   Second, what constitutes a cloud service for the purpose of the Bill requires further specificity.

   Noting that the Explanatory Memorandum describes cloud services (for the purpose of providing data storage and processing services) as including, Infrastructure as a Service (IaaS), Software as a Service

(SaaS) and Platform as a Service (PaaS), we believe there is a significant differentiation between IaaS and SaaS and PaaS such that SaaS and PaaS should not fall within this sectoral definition.

- SaaS and PaaS data storage and processing related risks are manageable via other control routes, including through application of the CAAF (as noted above), especially where these are hosted on a CAAF assessed IaaS.
- From a practical perspective, numbers of SaaS and PaaS providers impacted (likely to be in the tens of thousands) will make application and management/control of the Legislation complex and difficult. Alignment with the CAAF for the purpose of operationalizing critical infrastructure sector industries 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.

We recommend that the scope of the proposed legislative changes for cloud services, apply to the combined data centre, network systems, computing systems, storage systems and related operating systems (i.e. IaaS only as defined by NIST), with additional complexity (i.e. SaaS and PaaS services as defined by NIST) excluded.

For consistency with other Critical Infrastructure Sectors, we understand the need for an appropriate Regulator for the Data Storage and Processing Sector. Consideration should be given to what currently exists and appropriately requires further industry consultation given that proposed regulatory arrangements are yet to be defined.

4. **With recent changes introduced by the ACSC, IaaS is subject to best practice security assessment and compliance requirements in accordance with the CAAF. 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 largely align with the intent of the draft Legislation.**

Given that ASD (including ACSC) – as the designated ‘authorised agency’ (for the purpose of intervening to respond to a critical cyber security incident, in accordance with Part 3A), developed the endorsed best practice (i.e., the CAAF) in consultation with the technology industry, we believe the CAAF is the most appropriate benchmark. With the Explanatory Memorandum explicitly recognizing ASD as the Government’s ‘premier cyber expert’, the CAAF is implicitly endorsed as the expected standard of security for Government cloud services.

Further, these standards already apply to cloud and on-premise deployment of infrastructure and in many respects, also to data center operations. It would be practical that they become the default for the data storage and processing sector (as defined in the Bill) to mitigate risks to data in networks, storage and processing.

Noting the level of transparency of data flows and controls proposed by the CAAF (especially risks associated with sensitive/critical data moving off-shore), alignment with the CAAF will also reduce the risk of insider threats through the use of personnel who have been cleared in accordance with PSPF standards.

Therefore, for consistency of security assessment, management and compliance, consideration should be given to extending this best practice benchmark to other Critical Infrastructure sectors as it relates to data storage and processing. Application of the CAAF or IRAP where appropriate, would complement global regulatory standards. This also ensures that Australia's interests in terms of 'sovereign resilience' are the first order priority and not at risk of an 'uncontextualised' global standard that for the purpose of the intent of this legislation which applies to government and critical infrastructure, may be a lower standard.

This will also mitigate data storage and processing providers across all Critical Infrastructure Sectors, seeking to circumvent the Legislation by effectively operating their services or storing and processing data offshore which, under the terms of the proposed legislation, is technically possible.

Importantly, application of best practice consistently will also reduce the need for Government to invoke the intervention rights given to the Minister for Home Affairs, as outlined in the Legislation and Explanatory Memorandum. This would alleviate a major concern that some global providers have in relation to the direct action/intervention proposed in Part 3 of the Bill.

5. **Noting the proposed CAAF benchmark, and to ensure consistent security risk mitigation, where a Critical Infrastructure Sector organisation is operating an on-premise (or self-managed) environment, they should also be required to undertake and satisfy an IRAP assessment. Similarly, where a Critical Infrastructure organisation is migrating to the Cloud, those services should be assessed under the CAAF.**

   This aligns with the recommendations above, and is consistent with current Government data storage and processing requirements - with a new benchmark framework and process implemented only this year (the CAAF and renewed IRAP), supported by ongoing revisions to the ISM aimed to keep pace with the changing technology landscape, and specifically virtual data management and cloud services.

# Conclusion

As noted at the outset, AUCloud understands the broader context for, and the intent of this Draft Legislation. We believe 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 (the sum of the parts is more effective than the individual elements). For this reason, 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 and foundation of our democracy and livelihood of our citizens.