AIIA Submission to the Department of Home Affairs' Critical Infrastructure Centre's Consultation Paper: *Protecting Critical Infrastructure and Systems of National Significance*

About the AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for organisations in the digital ecosystem. Since 1978 AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for members and to contribute to Australia's economic prosperity.

We do this by delivering outstanding member value by providing a strong voice of influence; building a sense of community through events and education; enabling a network for collaboration and inspiration; and developing compelling content and relevant and interesting information.

Our members are diverse and truly represent the diversity of the Australian tech ecosystem and include: Australian SME's and larger technology, telecommunications and infrastructure and cloud companies as well as hyper-scale cloud and multi-national software and SAS providers.

We welcome this opportunity to respond to the Consultation Paper on a very important policy reform that affects our industry and members.

Summary of recommendations

1. The AIIA has concerns around the process and speed to legislate: recommend government engage in further industry consultation and get details right. Support substantive Exposure Draft industry consultation process.
2. Be clear around the definition of Data and the Cloud and who is captured.
3. Recognise that Data and the Cloud is both a defined critical industry but also an industry horizontal when designing sector regulations and ensure consistency across sectors.
4. Base any Positive Security Obligations on international security compliance standards and best practices.
5. When naming an entity in regulations, define to business platform level.
6. Narrow and limit direct action powers.
7. Remove future proposed reporting of information requirement to a stand-alone process.
8. Include a legislated review of Act and conduct economic impact assessment post implementation.

Introduction

The AIIA is concerned that an important and indeed critical area of policy is being rushed through to legislation in the next few months when industry has a number of concerns and questions around the detail, scope and remit of the proposed expansion as well as the operation of new direct action powers. We believe more industry consultation is required and welcome the opportunity to provide comment on the Exposure Draft legislation once it is made available.

The AIIA does support the intent of the expansion of the definition of critical industries (CI). This review of critical industries and infrastructure and the consultation paper recognises the digitisation

of our economy and resultant cyber threats we are facing. However, given this importance to get it right, we believe that the economic impact assessment and both cross industry and individual CI standards work should be completed prior to passing legislation. Policy transparency is vital for industry and community support.

We do not accept that the threat of non-action exceeds the threat of unintended consequences and potentially poor drafting. Further, the Department of Home Affairs advised in an industry briefing that the legislation will not come into effect until specific industry standards are drafted and finalised. This raises the question: why not complete this work up front as this would enable Government and Parliament (as well as industry) to undertake a comprehensive assessment of the regulatory impact of the proposed changes to the large, medium and small businesses that may be captured by the reforms (and currently struggling in a once-in-a-lifetime economic event).

Our concerns centre around the definition of the proposed Data and the Cloud Critical Industry (**CI**) and the direct action proposal and is the focus of our submission.

Definition and scope of Data and the Cloud

The expansion of the CI and ES (essential services) demonstrates the critical role that digital technologies play in our economy. The inclusion of Data and the Cloud as a critical industry is sensible and supported by the AIIA.

However, the definition of the Data and the Cloud category in the legislation needs to be made clear so that industry can understand to whom the positive reporting obligations fall, and so the impact of the compliance costs be fully understood.

Data and the Cloud more specifically can be defined by three broad and well-understood categories: Infrastructure as a Service (Iaas), Platform as a Service (PaaS) and Software as a Service (SaaS) under NIST definitions.

The AIIA suggests that the legislation should clearly define to whom the positive security information and reporting obligations apply and that this should be restricted to IaaS providers.

Some limited PaaS and SaaS entities may be at such a scale across our economy and embedded in business and government systems that they meet a threshold of economic or national sovereign significance, but these thresholds and determinations should be made when looking at each industry sector within the critical industries standards development by the sector regulator. Alternatively, these cloud solutions or platforms may be small in scale but play a vital role for a CI so again this should be determined by the specific CI.

In this context, it is important to note that “data” is in and of itself is not a sector. Likewise, the Cloud is only one of many technology service models that interact with data. Other models, including on-premise data processing and data storage, provide CI entities with options for managing the processing, hosting or storage of data. Any positive security obligations should be considered for these different models in an equivalent manner.

Given the complexity and broad definition of “Cloud”, the regulatory intent for Cloud Service Providers (CSPs) must be clearly laid out and understood. CSPs have a wide variety of products and the breadth of their customers is vast, thus the build out of the sector specific guidance and framework for them must be a considered process. We recommend that Home Affairs first undertake the guidance and framework design for each sector and once the overlay of already existing regulatory onus for Data and Cloud is fully understood, the drafting on the Data and the

Cloud guidance can be undertaken. A thorough gap analysis of the proposed principles-based outcomes and contemplated measures should be assessed against existing obligations across the various sectors to which cloud providers offer services prior to any measures being finalised. This should ensure that the objectives of the government are met by avoiding unnecessary duplication and regulation.

As part of the consultation process, Home Affairs has advised it is the security of the data itself in physical infrastructure is its primary concern. As such, the AIIA suggests that the legislation needs to be clear and unambiguous in relation to this.

Positive Security Obligations

The AIIA supports the Consultation Paper when it states:

> *Regulators will continue to work with entities to co-design sector-specific requirements and guidance to ensure the PSO is applied, taking into account the needs and capabilities of each sector.* (p. 21)

The role of the cross-industry sectoral regulations and standards as well as specific sectoral standards for named critical industries will form an important process and represent the appropriate place for determining which cloud entities meet a threshold for positive reporting under the scheme.

We support the desire of Government and the Department of Home Affairs to engage in co-design with industry to ensure the regulatory requirements are standardised as much as possible, avoiding unnecessary overlap, duplication and complication.

The role of the cross-industry sectoral regulations and standards as well as specific sectoral standards for named critical industries will be an important process and is the appropriate place for determining which cloud entities meet a threshold for positive reporting under the scheme.

It would be prudent that any PSO is based on international security compliance standards and best practices (i.e. for data centers: ISO27001 Series, SOC 2 and PCI DSS). Well regarded International Standards such as these will ensure that there is independent and constant review of the applied security framework, which in turn will ensures the ongoing state-of-the art protection for Australia's CI.

With this in mind, we support the desire of Government and the Department of Home Affairs to engage in co-design with industry to ensure the regulatory requirements are standardised as much as possible avoiding unnecessary overlap, duplication and complication.

Data and the Cloud named entity application across a business

The Government, when defining Data and the Cloud to IaaS providers (and if the provider is a named entity in regulations), also needs to ensure that when making a determination it applies only to that IaaS and not the company (entity) as a whole. A large technology company may have multiple software and cloud offerings and only the IaaS service of that entity should be captured by the scheme and named in regulations and not the entire suite of service offerings (or company as a whole).

Initiative 3: Cyber Assistance for Entities

Under this proposal, Australian-based companies can be the subject of direct action by government:

> *In an emergency, we see a role for Government to use its enhanced threat picture and unique capabilities to take **direct action** to protect a critical infrastructure entity or system in the national*

interest. These powers would be exercised with appropriate immunities and limited by robust checks and balances. The primary purpose of these powers would be to allow Government to assist entities take technical action to defend and protect their networks and systems, and provide advice on mitigating damage, restoring services and remediation. (p. 29)

It is important that when government, via the Australian Cyber Security Centre (ACSC) considers direct action is required, that its request or action is directed at the organisation (i.e. business and industry) that is subject to the cyber threat. To make this clear, the IaaS, PaaS or SaaS provider should not be the target of the direct action by government. The organisation or business that is under cyber attack is best placed to understand which systems are being threatened, whether they have a hybrid cloud environment covering on-premise and multi-cloud environments and how their business operates. Further, contracts between cloud providers and their clients restrict their abilities by law to intervene in their client systems and data.

When designing a cyber-resilient environment for our critical industries including Data and the Cloud, the government may care to give consideration to developing a framework or model with industry that differentiates or recognises the maturity and capability of different providers. Many IaaS providers have deep cyber expertise and understanding, whilst there may be some smaller niche players that have limited resources and capabilities. A system that seeks to uplift the supply chain and remove the weakest vulnerability would be a sensible approach, drive stated policy outcomes and focus scarce government resources.

The AIIA understands that the Government is seeking to also address “unicorn” or extreme cyber attack events that threaten entire cloud environments in a “worst-case” scenario and wishes to reserve the right to intervene. AIIA recommends that in this instance direct action application to IaaS providers should have:

- limits on the powers of Commonwealth officers working with private sector operators, including bans on conducting cyber offensive activities from within private sector infrastructure;
- a high threshold under which such directions power can be issued;
- a requirement for independent authorisation of such power; and
- time limits on such powers.

Further, the legislation should also be clear on what is out-of-scope under this direct action power as per the first point above, explicitly ruling out that the government has no intention to conduct offensive cyber campaigns within the network of an IaaS.

Concerns over PSO requirements and access to information

Already, most of the larger data and cloud IaaS service providers share cyber threat intelligence and vulnerability data under current government arrangements and have a high level of transparency to government, and support this arrangement continuing. Under the Information Security Registered Assessors Program (IRAP) program the government also currently has a high level of visibility of security controls and operations. This current arrangement should continue.

The ACSC needs to work through the cloud providers’ customers and develop industry sector standards to uplift threat reporting and compliance rather than legislating a blanket enforceable obligation “to provide information about networks and systems”. The reporting should be undertaken by the customers, who have a complete view of their own systems, than be required of the cloud service providers.

The Consultation paper refers to a future ambition or requirement around reporting of data direct to government:

> *In the longer term, owners and operators of systems of national significance will be obligated (under amendments to the Act)* ***to provide information about networks and systems*** *to contribute to this threat picture if requested. When a request is issued, it will include the format the information is required in (up to and including near real-time), as well as a specified timeframe to work with the Government to provide the information. At present, we do not anticipate that all owners and operators of systems of national significance will be requested to provide such information.* (p. 26).

It is unclear to the AIIA what these future requirements may be and we propose that any legislation omits this "longer-term" obligation, as this can be dealt with by legislative amendment should it be required in the future. We also propose a scheduled legislative review by Parliament (see next section) of the Act so this issue can be captured through that future review process in a more considered fashion.

Legislated review and economic impact assessment

The AIIA would like a review of the legislation built into the amendments. We suggest this takes place two years after the Act comes into affect. We further suggest that the Government be required to undertake an economic impact assessment on the introduction of the scheme so government can more accurately measure the costs of the expansion with the benefits and better understand whether amendments need to be made in either scope or reporting.

For further information please contact:

Simon Bush

GM, Policy and Advocacy

AIIA

E: [redacted]