27 November 2020

Department of Home Affairs
Commonwealth of Australia

RE: SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020

Amazon Web Services ("**AWS**") welcomes the opportunity to make a submission on the Australian Government's *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (the "**Bill**"). We support the Government's objective of building on existing requirements in the *Security of Critical Infrastructure Act 2018* (the "**Act**") and introducing an enhanced regulatory framework to uplift the security and resilience of Australia's critical infrastructure.

One of our highest priorities is working with our critical infrastructure customers and the Australian Government to help develop a framework that uplifts security across the board. We believe this can be done while also prioritising the protection of the most business-critical components of Australia's infrastructure, and ensuring that any regulatory requirements and compliance costs are practical and manageable.

We attach to this letter a submission that lays out in detail our comments and feedback on the Bill. Our submission comprises the following sections:

1. **Summary Position**: outlining our core concerns and why we believe this Bill should be refined further to ensure its framework is appropriately scoped, ensures consistency and coordination across regulated sectors, and balances the objective of uplifting the security and resilience of critical infrastructure with appropriate guardrails and oversight.
2. **Key Issues with the Bill**: detailing the specific issues we have with the Bill, explaining our reasoning for these concerns, and outlining our recommendations to resolve those issues.
3. **Appendix A**: **Summary Table of Recommendations**: replicating our recommendations in tabulated format.
4. **Appendix B**: **Introduction to AWS**: explaining what AWS provides for our customers and outlining our basic cloud computing business model for background.

We welcome the opportunity to engage and cooperate with the Government further in the development of this enhanced regulatory framework.

Best Regards,

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

SUMMARY

AWS delivers services to millions of customers in Australia and worldwide, including commercial enterprises, entities that provide essential and critical services, and government agencies. Security is our top priority. Our customers trust us to handle their data securely, and we honour our commitment to build and operate infrastructure that satisfies the requirements of the most security-sensitive organisations. We therefore stand as one with the Australian Government in our commitment to cyber security, and are delighted to partner with the Australian Government in building enhanced regulatory frameworks to improve the resiliency and security of all Australian critical infrastructure.

We recognise the intention of the Bill is to set out a broad legislative framework that enables critical infrastructure regulators to develop more detailed sector-specific rules and guidelines at a later stage, after extensive consultation with industry and regulated entities. We believe the starting point for any effective legislative framework is appropriate scoping and prioritisation - without these, regulators and regulated entities will struggle to identify and protect critical infrastructure assets.

To achieve an appropriate scoping of the Bill we strongly believe ***all* data storage and processing facilities must be secured to the same high level – regardless of whether a critical infrastructure entity chooses to manage, process, host, or store data in the public cloud, in third-party data centres, "on-premise" within its own data centres, or in some other "hybrid" model**. In other words, the same rules should apply to all use of Information Technology, if it is deemed part of a critical infrastructure entity or operation. We have therefore made recommendations that the Bill should adequately address the full scope of assets and entities that store or process data. We propose the Government do this by (i) simplifying the definition of a "critical data storage or processing asset" and (ii) regulating –assets that store or process "business critical data" regardless of whether those assets are used to provide a commercial service to others - thereby ensuring that all of these critical assets attract a Positive Security Obligation.

We are also concerned that **the Bill imposes undue regulatory burdens and costs on regulated entities in some areas due to a lack of appropriate scoping**:

- Firstly, the proposed definition of "asset" - which is non-exhaustive and includes non-physical assets, such as "computer programs" and "computer data" - extensively expands the scope of the Act beyond its original focus on regulating physical facilities, supply chains, information technologies, and communication networks. This introduces significant commercial risks for companies because under the Bill, the Government could direct a regulated entity to do essentially anything in relation to any of these assets, or could even intervene directly in the handling of that asset. For example, the Government could mandate alterations to computer programs and regulate how data can be processed or stored. This represents a disproportionate and significant overreach on the part of the Government and fails to recognise regulated entities' existing legal and contractual commitments, including those relating to intellectual property and commercial secrets.
- Secondly, the definition of "relevant impact" - in so far as it relates to a cyber security incident - and the framework for notifiable cyber security incidents are impracticable and will result in over-reporting.

Collectively, these additional regulatory burdens are disproportionate. They introduce significant commercial risks and costs, and are counter-productive for security as they do not enable regulators and regulated entities to focus on identifying and addressing systemic risks and serious cyber security incidents.

Additionally, **the Bill has the potential to impose an undue burden on the data storage or processing sector if regulatory requirements in this sector overlap or are inconsistent with other regulated sectors**. The scope of regulation for this sector depends entirely on whether the end-user of a data storage or processing asset is a regulated critical infrastructure entity in one of the other regulated sectors that is storing or processing "business critical data", or a public sector end-user. Due to the potential for overlapping regulations and the fact that many customers across sectors will use the same data storage and processing services, there is a high likelihood that the

data storage or processing sector could be subject to the regulations and responsibilities of *all* regulated sectors simultaneously.

We believe it is vital that this risk of overlap is addressed at the legislative drafting stage, as this will provide Government and sector regulators clear swim lanes and guidance from the outset. It will also provide the Government the necessary legislative backing to de-conflict requirements between the different regulated sectors in the implementation phase. We have therefore made recommendations on how to apply Positive Security Obligations consistently, and to streamline compliance and regulation by ensuring that regulated entities are only required to comply with a single set of clear, sector-specific requirements for each asset. Key among which is the recommendation that Government and *other* critical infrastructure sector regulators state that a critical data storage or processing asset's compliance with its own sector Positive Security Obligation is sufficient to meet any sector-specific Positive Security Obligations that require due-diligence or security reviews of their data storage or processing service providers or critical data storage or processing assets. This will ensure that the enhanced security of critical data storage or processing assets will uplift security and resilience in all *other* regulated sectors, without imposing unnecessary and additional compliance costs.

We also understand that **the Government is trying to achieve a complex balance through the proposed "assistance" powers to respond to serious cyber security incidents**. On the one hand, the Government must ensure that it has the necessary information to guide companies and provide threat analysis to raise an alert early, and offer assistance where it might be needed and desired. On the other hand, the Government can and should learn from and collaborate with global security experts, companies and service providers that have deep security knowledge, while providing them with the space and flexibility to secure their own infrastructure to the highest global standards.

In our view, the Bill does not appropriately strike this balance. The Bill's assistance and step in powers are defined generally enough to allow an unimaginably broad scope of interventions. This alarms us and many others in the community. Unlike voluntarily accepted assistance, the Bill also includes powers for the Government to literally order an entity to do any "act or thing" (anything). In addition to this, the Bill's contemplated rights allow the Government to "step in" and take control of assets across a broad range of Australian society. These expansions of powers are unprecedented in our experience and rife with unintended consequences and risks that are disproportionate to the ills they seek to cure.

In addition to the breadth of these powers, we are concerned by the lack of sufficient guardrails in the Bill - particularly in the areas of the Government's "assistance" powers and proposed Enhanced Cyber Security Obligations. This is troubling because, among other things, (i) it would enable the Government, under certain circumstances, to exercise its powers without consulting regulated entities; and (ii) it does not provide regulated entities with the ability to seek a review of the merits of the Government's use of "assistance" powers by a judge.

While we recognize the complex dilemma facing a Government needing to respond urgently to a cyber security incident, this lack of consultation with the regulated entity could lead to unintended consequences – for example, introducing security vulnerabilities into the regulated entities' infrastructure – which would would materially impact regulated entities, the data storage or processing sector, as well as any industry relying on a regulated entity's technology. This will counterproductively lead to a systemic weakening of cyber security. Considering that the Bill touches so many sectors, it is also troubling that the Bill does not allow a judge to review the merits of the Government's use of "assistance powers". This means to the extent any review is available, it will be limited to whether the Government's decision was made lawfully, and likely after an entity has complied with a direction under the threat of civil penalties or imprisonment. This lack of review is particularly concerning when coupled with the Bill's broad grants of powers that are triggered entirely by the discretionary judgments of individuals in Government.

And finally, we do want to reiterate our alignment with the Australian Government's broad objectives – we too want to see the Australian Government build enhanced regulatory frameworks to improve the resiliency and security of all Australian critical infrastructure. We also hope to closely partner with the Government to achieve those objectives. However, the proposed Bill does contain a number of concerning elements and we hope that our submission and feedback can be seen by the Government in the positive and constructive light it was intended.

KEY ISSUES AND RECOMMENDATIONS

1. GENERAL IMPACT OF THE BILL ON REGULATED ENTITIES

The Bill contains several problematic provisions which are overly broad and create uncertainty as to their scope of applicability. This could unnecessarily increase regulatory burdens and costs for regulated entities. Some of the proposed provisions are also impracticable, such as the amount of time provided for regulated entities to report cyber security incidents. If regulated entities are unclear of how or unable to comply with elements of the Bill, or if the timelines simply cannot be met practically, this will undermine the aim of the legislation because instead of uplifting security, it will decrease confidence of regulated entities in their ability to protect critical infrastructure.

Therefore, the Bill, if passed in its current form, will increase the cost and complexity of compliance for regulated entities. This will have knock-on effects on the broader economy, by making Australian critical infrastructure less safe, eroding trust in digital services and technology, and negatively impacting regulated entities. Below we recommend a set of changes that would make these provisions more targeted, achievable and unambiguous.

1A. The definition of an "asset" includes a non-exhaustive list of physical and non-physical assets (section 5).

The Bill defines an "asset" which is subject to regulation and provides a list of examples (i.e., a system, network, facility, computer, computer program, computer data, or "any other thing"). However, the non-exhaustive, open-ended nature of this definition raises a number of concerns, especially as there was no general definition of "asset" in the original Act but rather, a more sector-specific definition of "critical assets." The inclusion of a novel, sector-independent definition of "assets" invites uncertainty and could be interpreted as signalling an intention to expand the application of the Act beyond its original scope of regulating physical facilities, supply chains, information technologies, and communication networks.

The new definition would allow the Government to expand the application of the Act to regulate non-physical assets (e.g., computer programs or computer data) and would also give the Government broad discretion to classify "any other thing" as an "asset" to be regulated. In combination, these factors may enable the Government to regulate digital commercial services (i.e., computer programs) or proprietary data on those services (i.e., computer data). Once regulated, the Government, in the event of a serious cyber incident, could then use overly broad powers to direct an entity to do any act or thing, or assist the Government to directly intervene in that asset.

We submit this is an unacceptable risk to commercial entities. The definition's non-exhaustive scope and inclusion of non-physical assets is an overreach in regulation of commercial assets. We submit that the intended effect of the Bill - to uplift the security and resilience of Australia's critical infrastructure - will be watered down if the Government attempts to cover all assets, including computer programs and computer data, within regulated sectors, especially considering the clear difficulty in regulating such assets across broad swathes of the Australian economy in a one-size-fits-all manner. Importantly, the definition may also significantly reduce how confident regulated entities are in their ability to protect their assets and services from undue Government interference. In turn, this could affect businesses' and every day Australians' confidence in the safety and security of commercial services provided by these regulated entities. In short, reining in the definition of assets to be regulated would both help address concerns raised by the Bill and improve the likelihood the Bill achieves its objectives.

Recommendation 1A - Amend the definition of an "asset" in the Bill by (i) deleting any references to non-physical assets (e.g., computer programs and computer data), (ii) ensuring that an "asset" is limited only to physical infrastructure (e.g., a "physical system" or "physical network"), and (iii) ensuring the list of examples is exhaustive, including the deletion of limb (i) of the definition (i.e., "any other thing").

1B. The definitions of "relevant impact" of a cyber security incident (sections 8G(2), 12P, 30BA to 30BD, 30CJ, 30CN, and 30CS) and "unauthorised access" (section 12N) need to be clarified.

The terms "relevant impact" (section 8G) and "unauthorised access" (section 12N) play critical roles in determining responsibilities and powers in the Bill, including those regarding the notification of cyber security incidents, the issuance of incident response plans, and the ability for the Minister for Home Affairs (the "**Minister**") to direct actions and gather information. However, as drafted, these definitions are ambiguous, are too easily triggered, and will lead to unnecessary confusion, over-notification, and increased compliance costs.

As drafted, it is unclear whether a cyber security incident that affects only small or isolated portions of a critical infrastructure asset would be considered to have a relevant impact on the asset. We submit it should not. As applied to the data storage or processing sector, only an impact that affects the service provider generally (e.g., affecting all customers of the service provider), or alternatively an entire region or service offering broadly (e.g., affecting all or substantially all of customers of the region or service) should be considered relevant. Additionally, given the intention of the Bill is to protect against cyber security threats – that is, threats initiated against the asset or entity by a third party with malicious intent – we strongly believe the meaning of a relevant impact should be clarified to only cover impacts to the availability, integrity, reliability, or confidentiality of the asset that are a direct result of a third-party malicious action.

A cyber security incident affecting only a portion of the critical infrastructure asset, or few customers, should not be considered to have relevant impact on the asset. Such an incident is frequently the result of customer misconfiguration or mismanagement, rather than systemic vulnerabilities, and does not create the type of interconnected risk that the Bill is intended to address. Triggering responsibilities and government powers in response to such an incident creates unnecessary obligations on data storage or processing providers, may cause unnecessary concern among unaffected customers, and would not increase safety. Further, existing laws will already require notices for specific types of data, and those laws are drawn in a manner that is appropriately tailored to the data. This new overarching law will duplicate obligations if applied below the level where the impact of the incident is not systemic.

For example, if an affected customer is a regulated critical infrastructure entity, and the workload in question constituted "critical business data," then a cyber security incident could have relevant impact to that customer. In such a case, unless otherwise agreed between the critical infrastructure entity and their data storage or processing service provider, we expect that the customer would provide appropriate notification to their relevant critical infrastructure sector regulator.

Recommendation 1B(i) - Amend the Bill to clarify that (i) a cyber security incident has a relevant impact only if there is systemic or broad impact to the relevant critical infrastructure asset, and (ii) a relevant impact must be an impact to the availability, integrity, reliability, or confidentiality of an asset that is a direct result of a third party's malicious actions.

While we do not believe that this is the intention of the Bill, the definition of "unauthorised access" could be interpreted to include access by internal personnel not "authorized" but nevertheless permitted to access an asset due to over-permissive access management policies. Misconfigured or misapplied internal policies, while problematic, do not create the type of systemic risk that the Bill seems intended to address, such as those posed by malicious third parties. Failing to clarify this point could result in entities designating routine internal issues as cyber security incidents, leading to over-reporting and increased compliance burden with no real decrease in systematic risk.

Recommendation 1B(ii) - Amend the Bill to clarify that "unauthorised access" only includes access originating from an unintended third party with malicious intent (section 12N).

The Bill should also recognize potential shared security/responsibility models when determining responsibility for notifying of cyber security incidents. The shared security/responsibility model is a common framework in cloud computing that divides responsibility for security between the cloud services provider and its customer. The cloud services provider is responsible for "security of the cloud," which typically includes the infrastructure that run cloud services, and the customer is responsible for "security in the cloud," which typically includes configuration of the

services it uses, who can access the data it stores, and whether the data is encrypted. Please see Appendix B page 24 for more detail on the AWS shared responsibility model.

The Bill should provide that a cyber security incident only occurs in respect of a data storage or processing services provider or its customer when the incident occurs in their respective areas of responsibility. This distinction is necessary because some data storage or processing service providers and their customers lack visibility into the choices made by the other party. For example, a cloud services provider could not effectively assess whether its customer authorized any particular person to access its data, intended to delete data previously stored in the cloud, or chose to deliberately take a resource offline. The cloud services provider and its customer are the only ones equipped to assess and mitigate a potential cyber security incident occurring in their respective areas of responsibility, and they should bear responsibility for addressing cyber security incidents accordingly. This clarification should be made in the Bill rather than left to sector regulators because it is fundamentally important to having a workable cross-sector regulation.

Recommendation 1B(iii) - Amend the Bill to clarify that a cyber security incident only occurs in respect of a data storage or processing services provider or its customer when the incident occurs in their respective areas of responsibility.

1C. Ensure there is sufficient time for an entity to notify the Government of "confirmed" cyber security incidents. (sections 30BA to 30BD).

While we agree with the proposed approach for the two-tiered security incident reporting system provided in Sections 30BA to 30BD, we are concerned that the reporting time frames are impractical and too short.

We recommend triggering the deadlines associated with critical cyber security incidents (section 30BC) and other cyber security incidents (section 30BD) off confirmation of an incident with significant or relevant impact (as appropriate), rather than awareness that one may have occurred. We also recommend giving entities 72 hours after such confirmation to make the report. Once aware of a potential issue, service providers typically identify the cause of the problem, recreate it, determine the scope of potentially affected customers, and start to mitigate the harm to customers. A deadline that begins on awareness is likely to distract from this time-sensitive and critical work and may require service providers to provide incomplete reports just to meet the deadline. Additionally, service providers understandably want their reports to be accurate because inaccurate reports risk causing unnecessary concern and reputational harm. Giving service providers sufficient time to investigate and compile the facts will facilitate higher quality reports while also appropriately prioritizing customer needs in the immediate aftermath of the incident.

We also recommend that the Government allow responsible entities to comply with notification requirements via "public" disclosure mechanisms like AWS' *Service Health Dashboard*,[1] which provides our most up-to-the-minute information on service availability on a publicly accessible dashboard providing information on service functionality. Allowing entities to use existing mechanisms that meet the goals of the Bill would reduce the burden of compliance while offering the Government a way to obtain relevant information quickly and efficiently.

Recommendation 1C - Amend the Bill to clarify that (i) the deadlines for critical cyber security incidents (section 30BC) and other cyber security incidents (section 30BD) are trigged on confirmation rather than awareness of an incident with significant or relevant impact, (ii) the time period for notification is 72 hours, and (ii) the Bill allows for public disclosure mechanism rather than additional prescriptive channels.

1D. Entities should only have to report generalized operational information

We are also concerned with the obligations the Bill will place on an expanded range of regulated entities to report highly confidential operational information about critical infrastructure assets in the Government's register of critical

[1] https://status.aws.amazon.com/

information (the "**Register**"). While we acknowledge that the Register is treated confidentially, and reported information is treated as protected information, we are concerned that the disclosure of operational details such as the location of particular assets (e.g., data centres), and descriptions of the arrangements under which certain data relating to an asset is maintained, will create incremental risks to a regulated entity's security and proprietary information. This is especially pertinent considering regulated entities do not have visibility into how the Government stores, secures, and allows access to, reported operational information.

We submit that the Government should accept generalised - rather than specific - operational information whenever possible, as we believe that specific information should only be requested to address cases of identified cyber security risks. For example, rather than requiring the address at which data related to a critical infrastructure asset is held internationally, the responsible entity should instead be allowed to provide the country, state, or city in which the data is stored along with the regulated entity (if appropriate).

Recommendation 1C - Amend section 7 of the Act to clarify that regulated entities are only required to report generalised operational information (inc., the general location of a critical infrastructure asset and a general description of the arrangements under which data relating to the asset is maintained)

2. SPECIFIC DATA STORAGE OR PROCESSING SECTOR CONCERNS

The Bill as drafted does not adequately cover the full scope of assets and entities in the data storage or processing sector. First, the current definition of a "critical data storage or processing asset" is unnecessarily broad and contains several ambiguities. Second, the exclusion of "non-commercial" entities from the sector definition creates the potential for a serious gap. This exclusion means the Bill fails to account for the need to future-proof this legislation and ensure that there are sufficient Government powers over a non-commercial entity that could be processing business critical data or public sector data – but that doesn't fall into one of the other regulated sectors. We submit these issues can be corrected by (i) including a more objective threshold in the definition of a critical data storage or processing asset (e.g., power capacity, which is the primary unit of measurement for all data centres), and (ii) the inclusion of non-commercial entities within the scope of the data storage and processing sector.

2A. The definition of "critical data storage or processing asset" needs to be simpler and more objectively specific (section 12F).

The definition of "critical data storage or processing asset" is unnecessarily broad. For example, an asset owned by a data storage or processing entity and used to provide data storage or processing services will become a critical data storage or processing asset if (i) any of those services are provided to an Australian government entity, even if the government entity's data being stored or processed is insignificant, or (ii) any of those services are provided to a responsible entity for a critical infrastructure asset and relate to business critical data, even if the data is only ancillary in nature or if its interruption, and therefore disclosure or interception would not have a material impact on any critical infrastructure asset. The combined effect would be to regulate all workloads of a regulated entity as though they require the highest level of protection and this will make all workloads more expensive, slower to innovate, and spread the attention of security teams too thin to prioritize truly critical assets.

The definition also contains several ambiguities and will likely be very difficult for data storage or processing sector entities to accurately apply. The term "wholly or primarily" in sections 12(1)(b) and 12(2)(b) of the Bill are vague, and might inadvertently exclude multi-purpose assets that store or process large volumes of business critical data but are not used *wholly or primarily* in connection with a data storage or processing service. The definition of "business critical data" is also vague and likely to be interpreted inconsistently by different data storage or processing sector entities. In addition, data stored or processed using data storage or processing services typically changes rapidly and it is impossible for a data storage or processing service provider to access or monitor this data, or for customers to notify data storage or processing service providers of all these changes.

The breadth and ambiguity of the definition will likely force most data storage or processing service providers in Australia to assume that *all* of their assets used in connection with data storage or processing services are critical data storage or processing assets. This in turn would stifle technology investment in Australia, because it will not be economical for data storage or processing providers to develop and launch new technologies or improvements of existing technologies if they must all immediately comply with Positive Security Obligations regardless of their scale and significance. It might also reduce access to innovative technologies for government and critical infrastructure customers.

To resolve these concerns, we reiterate our previous recommendation that the definition of a "critical data storage and processing asset" include a simple threshold (e.g., power usage or number of server racks) that is set relatively low for the data storage or processing sector. We think that a power threshold (e.g., 100kW) is likely to be both the simplest to apply and hardest to circumvent threshold. This threshold would ensure that the definition covers all assets of a size and scope likely to have a potentially significant impact, without inadvertently covering small and insignificant data storage or processing assets. We would further submit that this appropriately focuses on the physical assets rather than a vaguely expansive definition, as we discussed in Section 1A of this submission.

Recommendation 2A - Amend the definition of a "critical data storage or processing asset" in the Bill to include a simple threshold (e.g., power usage or number of server racks).

2B. Ensure that any asset that store or process "business critical data" are regulated as critical data storage or processing assets attracting the Positive Security Obligation, regardless of whether those assets offer services "on a commercial basis" to others (section 5) .

The Bill's definitions of the "data storage or processing sector" and "critical data storage or processing asset" focus only on entities that offer, and assets that support the provision of, commercial services. This singular focus creates a risk to the Government's ability to improve the security and resilience of all assets that may store or process business critical data. Specifically, it means that entities using their own assets to store or process business critical data (e.g., on premise data centres) will either not be regulated, or if regulated likely have to comply with Positive Security Obligations that are inconsistent with those in the data storage or processing sector.

We believe there is a very probable risk that non-commercial assets that store or process business critical data will not be regulated as critical infrastructure assets by other sector regulators. The Bill implies it will be left to other sector regulators, based on their own understanding of their sector and interpretation of the Bill, to determine if they need to develop sector-specific rules for these non-commercial assets. However, we believe that sector regulators are unlikely to do this because (i) no other definition of critical infrastructure assets in the Bill considers non-commercial assets that store or process business critical data, and (ii) these regulators will not necessarily have the knowledge or expertise to regulate these non-commercial assets. However, even if a non-data storage or processing sector regulator decides to create sector-specific rules for these non-commercial assets, they are still likely to apply these rules in a way that is inconsistent with those applied to commercial assets in the data storage or processing sector. This would be because they either developed their sector-specific rules in isolation, or because they choose to partially duplicate sector-specific rules from the data storage or processing sector.

These issues create the potential for a weak link in the chain of securing all business critical data. The resiliency of critical infrastructure assets and the security of business critical data is dependent on ensuring that *all* data storage and processing assets – commercially sold or otherwise - are secured to a consistent high level (i.e., regardless of whether an entity chooses to store or process data, whether in the public cloud, in third-party data centres, or on premise within its own data centres).

From our perspective, it is clear that the use of cloud services like AWS would generally improve the security of Australian entities that are using on-premise data centres. If this gap is not addressed, the Bill could undercut its own objectives by incentivizing entities to continue using less secure on-premise data centres to avoid incremental regulatory burdens or interventions. Further, as entities are transitioning to the cloud, they could find themselves subject to different requirements depending on the service models they are using for different parts of their

operations. These harms can be avoided by changing the scope of the Bill to apply evenly to all critical data storage and processing assets rather than distinguishing based on whether those assets are used to power a commercial offering.

Recommendation 2B - Amend the Bill to include non-commercial entities and assets in the definitions of the "data storage or processing sector" and "critical data storage or processing asset" (section 5).

3. CONCERNS AROUND CONSISTENT APPLICATION OF POSITIVE SECURITY OBLIGATIONS

The Bill does not include provisions to address challenges that may emerge when regulated sectors interact with each other – particularly when regulated data and storage sector entities act as the service provider for regulated entities in the other regulated sectors. Inconsistencies in the implementation of Positive Security Obligations would create a significant security risk, increase compliance costs and administrative burdens, and not achieve the Government's broader aims of uplifting security and resilience of all critical infrastructure. Additionally, the lack of clarity around whether regulated entities could be subject to oversight by multiple regulators and the ability for the Government to enact sector-wide rules without consultation creates significant uncertainty, and will decrease the confidence of regulated entities in their ability to protect their assets.

3A. Ensure that critical infrastructure entities only have to comply with one set of sector-specific requirements for each asset and create an avenue to escalate inconsistencies.

The Bill creates the potential for overlapping, inconsistent, and impractical regulations because it does not include an anti-overlap provision.

By creating new regulated critical infrastructure sectors, the Bill introduces a risk that multiple sector regulators will regulate a single entity, directly or indirectly. This could occur either because the entity has assets in multiple critical infrastructure sectors, or because other sector regulators either directly or indirectly (via a customer that is a responsible entity in another sector), flow down additional security obligations that would duplicate, conflict with, or unnecessarily add to, the data storage or processing sector's Positive Security Obligation.

3A(i). The only Positive Security Obligation that should apply to a critical data storage or processing asset is the Positive Security Obligation for the data storage and processing sector

This risk of overlap is particularly great for the data storage or processing sector, both for service providers and customers. The definition of a "critical data storage or processing asset" is largely dependent on whether any of our customers, or the "end-users" of our services are *responsible entities* for a critical infrastructure asset and are using our services to store or process business critical data. Many Australian companies operate their own data centre assets (on-premises).

While we understand the need for a sector-by-sector approach, we are concerned that overlapping regulations would lead to an unwieldy set of inappropriate security requirements and an unnecessary increase in compliance costs, without increasing security. These outcomes are avoidable, and the Government will still meet its aim of enhancing security of critical infrastructure assets if the Government adds a new anti-overlap provision to the Bill, clearly stating that only the most appropriate Positive Security Obligation and sector-specific rules will apply to each critical asset. The Bill should address two key situations of potential overlap.

Firstly, sector regulators should not impose separate requirements on critical data storage or processing assets, directly or indirectly, which duplicate or build upon the data storage and processing sector's Positive Security Obligation.

Secondly, companies whose primary business is in another critical sector (such as banking) might also own or operate their own data centre assets. We submit that it is most appropriate to apply the data storage and processing sector's

Positive Security Obligation to critical data centre assets, even if the owner or operator of the data centre also has critical assets in a different sector. That is, companies with operations in multiple critical sectors should comply with the data storage and processing sector's Positive Security Obligation in relation to their critical data centre assets, and the other sector's requirements in relation to their primary operations. This will more effectively ensure high security standards than requiring entities to apply a Positive Security Obligation designed for an entirely different type of assets (such as applying banking standards to data centre assets).

Recommendation 3A(i) - Amend the Bill to clarify that a regulated entity is only required to comply with the data storage or processing sector's Positive Security Obligations for critical data storage and processing assets.

3A(ii). Introduce a safe harbour regime for regulated entities when receiving services from compliant data storage and processing sector entities

There is also a risk of overlapping or inconsistent regulation if other sector regulators (such as the banking regulator) expect entities in those other sectors to flow their sector-specific requirements down to their service providers in the data storage and processing sector. Where a banking entity or other regulated entity is receiving services from a critical data storage and processing sector entity, the data centre assets will already comply with the most appropriate sector's Positive Security Obligations, will already be subject to oversight by the most appropriate sector regulator, and the enhanced security of those assets will uplift security and resilience in the *other* critical infrastructure sectors. It would impose unnecessary and additional compliance costs on the regulated customer if it was required to impose additional contractual commitments on the critical data storage and processing sector entity to meet banking or other sector regulations. Doing so would not increase security of the other sector.

Therefore, compliance by a critical data storage and processing sector entity with its own sector Positive Security Obligation should be deemed to satisfy the sector-specific requirements of all other sectors, in relation to services provided by a regulated data storage and processing sector entity. Any other sector requirements to flow down particular contractual terms or regulations, conduct due diligence or inspections, permit audits, conduct security reviews, or comply with other sector rules, should be taken to have been satisfied whenever purchasing services from a data storage and processing sector entity who is subject to the data storage and processing sector's Positive Security Obligation. In this way, the Bill could improve security while actually reducing the regulatory burden.

Recommendation 3A(ii) - Amend the Bill to add a safe harbour provision stating that a regulated entity that uses a data storage or processing entity that is subject to the Positive Security Obligation for the data storage and processing sector, will be deemed to have met its own sector-specific obligations in relation to use of that data storage or processing entity.

3A(iii). There is no process for regulated entities to raise inconsistencies across sectors

We also submit that the Government should ensure that the Bill includes a process to allow regulated entities to escalate and directly discuss with the Department of Home Affairs, if regulated entities believe that a sector-specific rule - either in their regulated sector or another regulated sector - may raise any of the risks or issues that we have listed above. We believe that this would provide regulated entities with a formal, clearly defined process that would allow them to raise concerns and not seek to solely rely on the Department of Home Affairs' best intentions to ensure uniform and consistent sector-specific rules across all regulated sectors.

Recommendation 3A(iii) - Amend the Bill to include a process for regulated entities to raise concerns to, and discuss with, the Department of Home Affairs if they believe that any sector-specific rule in any regulated sector will create an issue or concern.

3B. Remove the Government's ability to enact sector-specific rules without consultation (section 30AL).

We support the Government's proposal for sector-specific rules to be developed via extensive consultation with a sector's regulator and regulated entities. It is critical that this consultation process is allowed to occur since these

rules will cover a broad scope of obligations and compliance with them is likely to have a significant or material impact on an entity's business and operations.

However, we are concerned that the Bill allows the Minister to make a sector-specific rule without any consultation, in the event there is an imminent threat that a hazard will have a significant relevant impact on a critical infrastructure asset. Such rules would then have near immediate effect and may require entities to take rapid and costly action to ensure compliance (under the threat of civil penalties). While such rules must be reviewed by the Secretary of Home Affairs (the "**Secretary**") within 60 days of being made, the Minister is still only required to table the review's findings in each House of Parliament (i.e., the rule may continue indefinitely). Further, these concepts of imminent threats and significant impacts, are vague concepts that are left largely to the discretion of the Government.

This situation creates an unacceptable risk to regulated entities. The Bill would allow the Minister the ability to make a sector-wide rule, without consultation, that may last indefinitely irrespective whether the significant relevant impact that triggered the need for the rule actually occurred. This outcome is inconsistent with the Government's intention to develop sector-specific rules through extensive consultations. The result would be that, in order to comply with a rule, regulated entities may have to take significant actions - which could cover anything from physical security, cyber security, personnel security, or supply chain security risks - and do so quickly, even if compliance would have a material or significant impact on the entity's business, operations, or customers. A transitional period of six months may also not be sufficient time for complex businesses to implement compliance with rules made without consultation.

We submit that it is inappropriate for the Government to be able to unilaterally determine new sector-specific rules without extensive consultation and that allowing the Minister to do so will reduce regulated entities' confidence in their ability to appropriately consult with Government on overly onerous requirements before compliance is required.

Recommendation 3B - Delete sections 30AL(3) and 30AM of the Bill.

4. PROPOSED GOVERNMENT POWERS ARE TOO EXPANSIVE AND LACK SUFFICIENT GUARDRAILS

We are deeply concerned about the lack of appropriate guardrails around, and limitations to, the Government's ability to assist regulated entities in response to serious cyber security incidents, and in respect of the Enhanced Cyber Security Obligations for Systems of National Significance. The "step-in/Government intervention" powers are significantly broad, unprecedented, and rife with the potential for unintended consequences. Without providing appropriate avenues for judicial merits review, these assistance requirements could result in significant unintended consequences for the broad swathe of regulated entities if these powers are applied incorrectly. Also, in light of the Government's aim to expand the number of regulated sectors already covered by the Act, our concerns with these powers also echo concerns we have with the Minister's existing power under the Act to direct an entity to do, or not do, a specified thing to mitigate against a national security risk. We believe that the proposed powers under the Bill, and existing ministerial directions powers under the Act, lack sufficient guardrails as described below.

Furthermore, the ramifications if applied incorrectly to the data storage or processing sector would affect public and private sectors beyond just the regulated sectors – given that a wide range of public and private sector end-users rely on these data storage or processing services to operate and function. This could have immediate effects on the Australian economy. In the longer term, an unintended consequence would be the erosion of public trust in digital services, impacting the growth of the digital economy and innovation in Australia.

Recommendation 4 - Delete Part 3A of the Bill.

4A. The Government's powers to respond to serious cyber security incidents are too broad and should be removed and reconsidered in consultation with regulated sector entities (Part 3A).

Part 3A of the Bill gives the Government exceptionally broad powers to gather information, issue directions, or act autonomously to directly intervene in an asset. For example, the Government can independently determine there is a threat, independently determine not to consult with the regulated entity, independently determine what the regulated entity must do, and there is no recourse for a regulated entity to challenge these determinations before a judge on their merits. This package of independently exercisable and unreviewable powers is too broad, inconsistent with a healthy separation of powers, and should be fundamentally reconsidered. Most alarming is that the Government proposes an unprecedented power allowing it to step-in and directly intervene in an entity's operations to take whatever action it deems appropriate to respond to a serious cyber security incident. This power, which grants the Government near complete discretion to interfere in an entity's operations however it chooses – while forcing the entity to provide assistance under threat of civil penalties - is so hostile we believe it will have a seismic impact on regulated entities and may lead them to reconsider if they will own and operate assets in Australia. We also don't understand how, given the complexity of various assets, the Government could reasonably believe such step-in power could be implemented quickly, operate effectively, and still achieve the Government's aim. We submit that introducing these powers is likely to have a chilling effect on technology investment and the Australian digital economy and will undermine trust in service providers who operate in or from Australia.

We submit that the Government should remove Part 3A from the Bill, should consult industry and other relevant stakeholders to define what specific powers are needed to achieve its aims, and pass further legislation introducing those specific powers if necessary. We do not think that handing unfettered powers to the executive arm of government now is the answer.

If the Government disagrees and instead retains Part 3A, then at a minimum there must be clearer limitations and guardrails to address the most significant issues with these powers, which are laid out below.

4A(i). The powers give the Government overly broad discretion to direct a regulated entity to do any act or thing - under the threat of imprisonment (section 35AQ).

The Bill permits the Minister to direct an entity to take direct action and do any kind of act or thing, without limitation, to address a cyber security threat. An entity may be directed to do any act or thing that may have a material or significant impact on its business, operations, or customers, and non-compliance by the entity may be a criminal offence punishable by up to two years' imprisonment. On its face, an entity could literally be required to do *anything*. For example, this may result in situations where an entity is instructed to take direct action to alter its existing technology or services, or implement new technology or services that may have a catastrophic impact on its existing assets or services – and it must do so or otherwise risk imprisonment of company officers. An entity may also have to do this in the time and manner directed by the Minister, and even in situations where the Minister hasn't first consulted with the entity. This is an unacceptable position for any entity, particularly when the exercise of Government powers may be authorised and directed based on the subjective view of the Minister and is not subject to effective judicial oversight.

The Bill should instead include an exhaustive list of acts or things that an entity may be directed to do, so that the scope of the new powers is clear and affirmed by Parliament, and they are not handing over unfettered powers to the executive arm of government. Non-compliance with any directions should also not be treated as a criminal offence because the broad and discretionary power for the Minister to direct an entity to do anything, within any time, at whatever cost, under the threat of imprisonment is completely inappropriate because non-compliance will not necessarily be a direct or deliberate action to cause harm to Australian or Australian citizens. We submit that the law should not permit the Minister to order anything he or she wants and back that with the threat of imprisonment. Even on the balance of protecting cybersecurity, this goes too far.

4A(ii). Government may direct certain regulated entities to intercept communications or provide stored communications (sections 35AK, 35AQ, and 35AX).

There is a significant issue regarding the Government's approach to prohibiting certain directions when it uses a power to direct a regulated entity to respond to a serious cyber security incident.

Specifically, an entity may be directed to take direct action to do any act or thing, including to intercept communications or providing access to stored communications. While the Bill does include a prohibition that the Government cannot direct an entity to provide information, or assist the Government to directly intervene, if that direction would be prohibited under sections 7 or 108 of the *Telecommunications (Interception and Access) Act 1979*, there is no equivalent prohibition when the Government directs an entity to take direct action to do an act or thing to respond to a serious cyber security incident. It is unclear to us why the Government included this prohibition in all other powers - except the power to direct an entity to take direct action and do any act or thing. We submit any prohibition on a Government direction should be applied uniformly across all Government powers that can be used to respond to a serious cyber security threat.

This issue puts at risk the privacy and security of Australian citizens and would undermine Australian citizens' trust in the Government's balancing of privacy and security. We think this could create a range of deeply negative consequences in and for Australia by making the experience of Australians less safe, eroding trust in regulated industry services and technology, and negatively impacting Australian technology companies and the Australian economy.

4A(iii). Exercise of the powers depends on the Minister's subjective views and occurs without any judicial oversight (section 35AB).

The exercise of the powers depends on the Minister's subjective views and does not require prior authorisation from a judge. For example, the Minister may unilaterally authorise the use of Government powers based on his or her opinion that there is a material risk that a cyber security incident is likely to seriously prejudice the social or economic stability of Australia. An entity can be directed to take direct action or assist the Government to intervene based on the Minister's opinion that the use of a Government power is a practical and effective response to the cyber security incident, whether the entity is unable to take all reasonable steps to resolve the incident, whether compliance by the entity is technically feasible, and whether any directions would be a reasonably necessary and proportionate response to the incident.

The Bill should instead:

- Incorporate an objective standard, where the validity of a direction depends on whether the relevant conditions are satisfied, and not whether a person holds an opinion.

- Require prior judicial authorisation, so that an independent decision maker assesses those conditions. We do not think that requiring prior judicial authorisation for the use of Government powers would adversely affect the ability of the Government to exercise its powers when required. Judges frequently listen to and grant orders made on urgent applications.

- If prior judicial authorisation is not required, the decision to authorise use of the powers should be subject to judicial review on its merits so that a regulated entity can respectfully challenge decisions where these conditions have not been met.

It is important that the exercise of such broad and impactful powers is subject to a transparent process with strong checks and balances to protect entities and the Government and mitigate perceptions that such exceptional powers could be misused.

4A(iv). Use of any Government powers must be necessary, proportionate, practicable, and feasible (section 35AB).

The list of things that the Minister must consider before authorising the use of the powers is inconsistent. For example, when issuing a direction to provide information, the Minister must be satisfied that the direction is likely to facilitate a practical and effective response to the cyber security incident. However, when issuing a direction to take direct action or assist the Government to intervene, the Minister must instead be satisfied that the direction is reasonably necessary. Further, the Bill does not require the Minister to have any regard to the legitimate interests of the entity, even though compliance may have a material or significant impact on the entity's business, operations, or customers.

The powers should only be used if it is necessary, proportionate, practicable, and feasible to do so, and the decision maker should take into account the interests and perspectives of the relevant entity and those who rely on it.

4A(v). The Minister is not always required to consult with an entity before using a Government power (section 35AD).

The Minister does not always have to consult with the entity before using its powers or confirm with the entity that the use of the power will actually address the cyber security incident. For example, the Minister is not required to consult if delay would frustrate the effectiveness of the subsequent direction to the entity. Again, the determination that consultation would "frustrate" the effectiveness of the direction is left to the subjective view of the Minister and theoretically any question or comment could be frustrating to immediate unquestioned compliance. The Bill should instead require the Minister to consult first with an entity before using its powers, and the Minister should give weight to the entity's view on whether the use of the power will address the cyber security incident.

4A(vi). Entities may be directed to take action that harms their customers (section 35AB).

While the Bill does not allow the Minister to require an entity to take direct action that would constitute an offensive cyber action against a person directly or indirectly responsible for the cyber security incident, the Minister can require an entity to take direct action that may harm the entity's customers or others. For example, the Minister may require an entity to take direct action to turn off services, change the functionality of services, or even restrict particular categories or types of customers from accessing or using a service. The Bill should not allow the Government to direct an entity to take direct actions that would harm a third party, including a customer or end user of the entity's services. Instead, the Bill should specifically prohibit directions that would harm a third party

4A(vii). Government intervention is not required to be a last resort.

The Bill would allow the Minister to use the powers concurrently, and for example, issue directions to an entity to take direct action and to assist the Government's own direct intervention, at the same time. This is inconsistent with the idea that direct intervention by Government is the last resort. The Bill should clarify that the power to direct an entity to assist the Government's direct intervention is a true 'last resort' power that can only be authorised when an entity is unwilling or unable to comply with a Government direction to take direct action.

4A(viii). The Bill allows the Government to direct entities to take action, either inside or outside of Australia that may violate the laws of other countries that apply to that entity.

While the Bill only applies to critical infrastructure assets located inside Australia, it still allows the Minister to require an entity to take direct action, or assist the Government to intervene, either inside or outside Australia that may violate the laws of other countries in which the entity operates.

For example, an entity that collects and processes the personal data of data subjects in another country with strong data protection laws (e.g., the European Union and its General Data Protection Regulation, or "**GDPR**") could be put in an untenable position with respect to how it processes the personal data of data subjects from the other country. Compliance with this Bill could be deemed incompatible with various requirements of the GDPR (e.g., that the data processor implement technical and organisation measures to ensure an appropriate level of security). An example under the Bill may be if the Minister directs an entity to take direct action in response to a serious cyber security

incident and such action detrimentally affects the technical and organisational measures the entity has implemented to ensure an appropriate level of security when processing personal data.

When Australian law and these other laws applicable to an entity conflict, the entity would be left having to arbitrate between them or decide whose laws to violate, knowing that in doing so, the entity might risk civil penalties or imprisonment. The Bill does not include a defence to noncompliance with a direction if it requires an action, either in Australia or a foreign country, that would contravene the laws of that foreign country. The Bill should not require an entity to take action or provide assistance inside or outside Australia in a way that may violate the laws of other countries in which the entity operates, and should include a defence to noncompliance with directions on that basis.

4A(ix). The Minister can issue multiple, ongoing Ministerial authorisations without limit (section 35AG).

While the Bill states that Ministerial authorisations to use Government powers must not exceed 20 days, there is no limitation on the Minister's ability to issue new authorisations for the same cyber security threat, provided they merely "have regard" to the number of authorisations made in relation to the specific asset. The Minister can authorise the use of Government powers for an indefinite period of time, requiring compliance under threat of civil penalties or imprisonment, even if compliance may have a significant impact on an entity's business, operations, or customers. The Bill should ensure that Ministerial authorisations are appropriately time-bound and cannot be re-issued indefinitely.

4A(x). Relevant entities that own or operate an asset may not be aware when a Government power is used in relation to that asset.

The Bill allows the Minister to authorise the use of Government powers against one entity connected to an asset, without other entities that may also own or operate the asset being aware. For example, the Bill allows the Minister to direct any "relevant entity" of an asset – including any direct interest holder, responsible entity, operator, or managed service provider of the asset – to provide information, take direct action, or assist the Government to intervene directly. For example, this may allow the Government to authorise the use of Government powers against a "managed service provider" who only manages as aspect of the operation of an asset, without informing the responsible entity who may have the license, approval, or authorisation to operate the overall asset. The Bill should allow an entity that has to comply with a Government direction to be able to inform other entities that own or operate the relevant asset that they have been issued a Government direction which may impact the asset.

4A(xi). Entities cannot recover the cost of complying with a Government direction.

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.

4A(xii). Entities do not benefit from full immunities and indemnities when complying with a Government direction.

The immunities for compliance with Government directions are inadequate. Additionally, the immunities would not act as an indemnity (inc., for claims from third parties in a foreign country). Firstly, an entity is only immune when it complies with a Government direction to take direct action, but is not immune when it helps the Government to intervene. We do not understand the basis for this distinction. Secondly, an immunity granted by Australian legislation cannot protect an entity against claims brought outside of Australia (and, as noted above, binding directions can be given in Australia that may cause an entity to violate foreign laws that apply to it). An entity may be forced to choose between complying with conflicting laws in countries where they operate, and to bear the risk of claims arising from that. This is not a reasonable position to be placed in. The Bill should grant immunity to an entity that is directed by the Government and include an indemnity for any third-party claims that are caused by compliance with the Government's directions.

4B. The Government's ability to require compliance with Enhanced Cyber Security Obligations are too broad and lack sufficient guardrails

Part 2C of the Bill gives the Government exceptionally broad powers to impose burdensome obligations on an entity without adequate limitations or guardrails. For example, the Government can direct an entity to participate in a cyber security exercise without any consultation, permit a third party to do a vulnerability assessment on an entity's asset, or require an entity to install and maintain a specified computer program that it did not create, may not want, and which may impact the entity's operations.

We submit that the Government needs to amend Part 2C of the Bill to remove these powers and, if not, limit the Government's powers and discretion, and provide regulated entities with adequate guardrails, as laid out below.

4B(i). The Minister is not always required to consult with an entity before using a Government power, and certain decisions depend on the Minister's subjective views

The Bill is inconsistent about when the Secretary must consult with an entity before requiring compliance with an Enhanced Cyber Security Obligation. For example, while the Secretary must consult with an entity before requiring a vulnerability assessment or access to system information, the Secretary does not have to consult with an entity before requiring a statutory incident response plan or conducting a cyber security exercise. Even when the Secretary does consult, the Bill still allows them to make the final decision based on their subjective view and irrespective of whether the entity agrees.

Additionally, the Bill permits the Secretary to subjectively determine whether an entity is capable of complying with an Enhanced Cyber Security Obligation. For example, the Secretary can determine if he or she thinks an entity is capable of complying with a vulnerability assessment or is technically capable of preparing a system information report. If the Secretary thinks an entity is not capable, the Secretary has the ability to impose overly burdensome obligations on the entity such as allowing a third party to conduct a vulnerability assessment on the entity's asset or requiring the entity to install and maintain a specified computer program that it has not created, does not want, and which may have a significant impact on the entity's business or operations. The threat of introducing computer programs in the systems of data storage and processing entities, in particular, may have a chilling effect on the use of those entities' services and inadvertently create a perception they are less secure.

We submit that the Government should amend Part 2C of the Bill and ensure that the Secretary does not have such broad discretion to impose overly onerous obligations on an entity.

Recommendation 4B(i) - Amend the Bill to ensure that the Secretary must first consult, and seek the agreement of, an entity before requiring the entity to comply with an Enhanced Cyber Security Obligation.

4B(ii). Entities cannot recover the cost of complying 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.

Recommendation 4B(ii) - Amend the Bill to ensure that entities may recover their reasonable and actual costs of compliance with an Enhanced Cyber Security Obligation.

4B(iii). Entities do not 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 Cyber Security 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 Enhanced Cyber Security Obligation and include an indemnity for any third party claims that are caused by compliance with such obligations.

Recommendation 4B(iii) - Amend the Bill to ensure that entities can benefit from full immunities and indemnities when complying with an Enhanced Cyber Security Obligation.

4B(iv). The Government has overly broad discretion to impose onerous obligations.

The Bill allows the Secretary to subjectively determine whether to impose overly onerous obligations on an entity. Specifically, whether to allow a third party to conduct a vulnerability assessment on the entity's asset or require the entity to install and maintain a specified computer program. Unfortunately, the entity must comply with these obligations under threat of civil penalties. This is not a reasonable position. Compliance with these obligations may result in an entity having to give a third-party sensitive access to assets or facilities to enable a vulnerability assessment. Alternatively, the entity may have to install and maintain a computer program that it did not create, may not want, and which may impact the entity's operations (since installation could impact other assets or services, and would need to be rigorously tested). We submit that any ability for the Government to require an entity to assist a third party to conduct a vulnerability assessment on the entity's asset or to install or maintain a Government directed computer program must be removed from the Bill.

Recommendation 4B(iv) - Delete sections 30CW, 30CX, 30DJ, 30DK, 30DL, and 30DM from the Bill.

4C. Ensure that judicial merits review is available for all Government decisions and directions under Part 3A of the Bill.

The Bill limits the ability of an entity to challenge Government decisions and directions because they are not subject to administrative review. This is because the Bill excludes the application of the *Administrative Decisions (Judicial Review) Act 1977* and its "order of review" in relation to decisions made under Part 3A (Responding to Serious Cyber Security Incidents). The scope of judicial review would therefore be limited to whether the decision to authorise the use of a Government power and a subsequent direction to an entity to do an act or thing was made lawfully. The actual decision to authorise the use of the Government power or direct an entity to do an act or thing cannot be reviewed by a judge on its merits. To the extent any judicial review can be sought, this would also likely be retrospective (i.e., in practice it would only be obtained once the Minister has authorised the use of a Government power or directed an entity to do an act or thing, and the entity has already complied with the direction under the threat of civil or criminal penalties). Once a direction has been complied with, the potential consequences may not be rectifiable, even if a court later decides that the direction was issued unlawfully. We submit that it is inappropriate to limit the scope of judicial review in respect of such powers, and that they should be subject to a judicial process that explicitly provides for Ministerial authorisations or directions to be challenged in the courts (on an urgent basis if needed) and set aside before any compliance is required.

Recommendation 4C - Delete the amendment to paragraph (da) of Schedule 1 of the Administrative Decisions (Judicial Review) Act 1977.

APPENDIX A: SUMMARY OF RECOMMENDATIONS

S/N	Issue and Section in the Bill	Recommendation	Rationale
1.	**Definition of *"asset"*** (section 5)	Amend the definition of an "asset" in the Bill by (i) deleting any references to non-physical assets (e.g., computer programs and computer data), (ii) ensuring that an "asset" is limited only to physical infrastructure (e.g., a "physical system" or "physical network"), and (iii) ensuring the list of examples is exhaustive, including the deletion of limb (i) of the definition (i.e., "any other thing").	Proposed expanded definition introduces significant commercial risks for companies, as the Government can direct an entity to carry out practically *any* action in relation to any of these assets or intervene in the handling of that asset. This represents a disproportionate and significant overreach on the part of the Government and fails to address potential intellectual property, commercial secrets and contractual commitments of regulated entities.
2.	**Definitions of "relevant impact" of a cyber security incident** (sections 8G(2), 12P, 30BA to 30BD, 30CJ, 30CN, and 30CS) **Definition of "unauthorised access"** (section 12N)	We recommend the following changes: • Amend the Bill to clarify that (i) a cyber security incident has a relevant impact only if there is systemic or broad impact to the relevant critical infrastructure asset, and (ii) a relevant impact must be an impact to the availability, integrity, reliability, or confidentiality of an asset that is a direct result of a third party's malicious actions. • Amend the Bill to clarify that "unauthorised access" only includes access originating from an unintended third party with malicious intent (section 12N). • Amend the Bill to clarify that a cyber security incident only occurs in respect of a data storage or processing services provider or its customer when the incident occurs in their respective areas of responsibility.	The terms "relevant impact" (section 8G) and "unauthorised access" (section 12N) play critical roles in determining responsibilities and powers in the Bill, including those regarding notification of cyber security incidents, issuance of incident response plans, and the ability for the Minister to direct actions and gather information. The current ambiguity in definitions may lead to unnecessary confusion, over-notification, and increased compliance costs.
3.	**Time for an entity to notify the Government of "confirmed" cyber security incidents** (sections 30BA to 30BD)	Amend the Bill to clarify that (i) the deadlines for critical cyber security incidents (section 30BC) and other cyber security incidents (section 30BD) are trigged on confirmation rather than awareness of an incident with significant or relevant impact, (ii) the time period for	We are concerned that the security incident reporting time frames in Sections 30BA to 30BD are too short and are not practical.

S/N	Issue and Section in the Bill	Recommendation	Rationale
		notification is 72 hours, and (ii) the Bill allows for public disclosure mechanism rather than additional prescriptive channels.	
4.	**Obligation on an entity to report operational information** (section 7 of the Act)	Amend section 7 of the Act to clarify that regulated entities are only required to report generalized operational information (inc., the general location of a critical infrastructure asset and a general description of the arrangements under which data relating to the asset is maintained)	We are concerned that the disclosure of operational details such as the location of particular assets (e.g., data centres), and descriptions of the arrangements under which certain data relating to an asset is maintained, will create incremental risks to a regulated entity's security and proprietary information. This is especially pertinent considering regulated entities do not have visibility into how the Government stores, secures, and allows access to, reported operational information.
5.	**Definition of "critical data storage or processing asset"** (section 12F)	Amend the definition of a "critical data storage or processing asset" in the Bill to include a simple threshold (e.g., power usage or number of server racks).	The definition is unnecessarily broad and contains several ambiguities and will likely be very difficult for data storage or processing sector entities to accurately apply, which will likely force most data storage or processing service providers in Australia to assume that *all* of their assets used in connection with data storage or processing services are critical data storage or processing assets. This in turn might stifle technology investment in Australia, because it will not be economical for data storage or processing providers to develop and launch new technologies or improvements of existing technologies if they must all immediately comply with Positive Security Obligations regardless of their scale and significance.
6.	**Ensure that any asset that store or process "business critical data" are regulated as critical data storage or processing assets attracting the Positive**	Amend the Bill to include non-commercial entities and assets in the definitions of the "data storage or processing sector" and "critical data storage or processing asset" (section 5).	There is a probable risk that non-commercial assets that store or process business critical data will not be regulated as critical infrastructure assets by other sector regulators. This creates the potential for a weak link in the chain of securing all business critical data. The

S/N	Issue and Section in the Bill	Recommendation	Rationale
	Security Obligation, regardless of whether those assets offer services "on a commercial basis" to others (Section 5)		resiliency of critical infrastructure assets and the security of business critical data is dependent on ensuring that *all* data storage and processing assets - commercial or otherwise - are secured to a consistent high level
7.	**Critical infrastructure entities should comply with only one set of sector-specific requirements for each asset and have an avenue to escalate inconsistencies** (new inclusion)	We recommend the following changes: • Amend the Bill to clarify that a regulated entity is only required to comply with the data storage or processing sector's Positive Security Obligations for critical data storage and processing assets. • Amend the Bill to add a safe harbour provision stating that a regulated entity that uses a data storage or processing entity that is subject to the Positive Security Obligation for the data storage and processing sector, will be deemed to have met its own sector-specific obligations in relation to use of that data storage or processing entity. • Amend the Bill to include a process for regulated entities to raise concerns to, and discuss with, the Department of Home Affairs if they believe that any sector-specific rule in any regulated sector will create an issue or concern.	The Bill creates the potential for overlapping, inconsistent, and impractical regulations because it does not include an anti-overlap provision. This risk of overlap is particularly great for the data storage or processing sector, as the definition of a "critical data storage or processing asset" is largely dependent on whether any of our customers, or the "end-users" of our services are *responsible entities* for a critical infrastructure asset and are using our services to store or process business critical data. We are concerned that this would lead to an unwieldy set of inappropriate security requirements, and an unnecessary increase in compliance costs, without increasing security. The Government should therefore avoid having sector regulators impose separate requirements on critical data storage or processing assets, directly or indirectly.
8.	**Remove the Government's ability to enact sector-specific rules without consultation** (section 30AL)	Delete sections 30AL(3) and 30AM of the Bill.	We think it is critical that this consultation process is allowed to occur since these rules will cover a broad scope of obligations and compliance with them is likely to have a significant or material impact on an entity's business and operations. Even in the event of an "imminent threat", the ability for the Minister to make sector-wide rules without consultation creates an unacceptable risk to regulated entities. The result would be that regulated entities may have to take significant actions to comply with a rule and do so quickly even if compliance would have a material or significant impact

S/N	Issue and Section in the Bill	Recommendation	Rationale
			on the entity's business, operations, or customers. We submit that it is inappropriate for the Government to be able to unilaterally determine new sector-specific rules without extensive consultation.
9.	**Government's powers to respond to serious cyber security incidents should be removed and reconsidered in consultation with regulated sector entities** (Part 3A)	Delete Part 3A of the Bill.	The powers under part 3A are too broad and give the Government exceptionally broad powers to gather information, issue directions, or act autonomously to directly intervene in an asset without adequate limitations or guardrails. The Government should remove Part 3A from the Bill, consult industry and other relevant stakeholders to define what specific powers are needed to achieve its aims, and pass further legislation introducing those specific powers if necessary.
10.	**The Government's ability to require compliance with Enhanced Cyber Security Obligations are too broad and lack sufficient guardrails** (Part 2C)	We recommend the following changes: • Amend the Bill to ensure that the Secretary must first consult, and seek the agreement of, an entity before requiring the entity to comply with an Enhanced Cyber Security Obligation. • Amend the Bill to ensure that entities may recover their reasonable and actual costs of compliance with an Enhanced Cyber Security Obligation. • Amend the Bill to ensure that entities can benefit from full immunities and indemnities when complying with an Enhanced Cyber Security Obligation. • Delete sections 30CW, 30CX, 30DJ, 30DK, 30DL, and 30DM from the Bill.	The Bill is inconsistent about when the Secretary must consult with an entity before requiring compliance with an Enhanced Cyber Security Obligation and permits the Secretary to subjectively determine whether an entity is capable of complying with an Enhanced Cyber Security Obligation. This could result in the imposition of overly burdensome obligations on the entity – such as allowing a third party to conduct a vulnerability assessment on the entity's asset, or requiring the entity to install and maintain a specified computer program that it has not created, does not want, and which may have a significant impact on the entity's business or operations. In such circumstances, the entity should have an avenue to be consulted on and be able to agree to the changes. Part 2C of the Bill should be amended to ensure that the Secretary does not have such broad discretion to impose overly onerous obligations on an entity.

S/N	Issue and Section in the Bill	Recommendation	Rationale
11.	**Judicial merits review should be available for all Government decisions and directions under Part 3A of the Bill** (new inclusion)	Delete the amendment to paragraph (da) of Schedule 1 of the Administrative Decisions (Judicial Review) Act 1977.	The Bill limits the ability of an entity to challenge Government decisions and directions because they are not subject to administrative review. It is inappropriate to limit the scope of judicial review in respect of such powers, and that they should be subject to a judicial process that explicitly provides for Ministerial authorisations or directions to be challenged in the courts (on an urgent basis if needed) and set aside before any compliance is required.

APPENDIX B: ABOUT CLOUD COMPUTING AND AMAZON WEB SERVICES

What is Cloud Computing?

Cloud computing is the on-demand delivery of compute power, data storage, database services, application development/deployment services, and other IT resources through a cloud services platform via the Internet with pay-as-you-go pricing. Whether customers are running applications that share photos to millions of mobile users or supporting the essential operations of their business, a cloud services platform provides rapid access to flexible and low-cost IT resources. With cloud computing, customers don't need to make large upfront investments in hardware and spend a lot of time on the heavy lifting of managing that hardware. Instead, customers can provision exactly the right type and size of computing resources they need to power their newest bright idea or operate their IT department. Customers can access as many resources as they need, almost instantly, and only pay for what they use. Cloud computing provides a simple way to access servers, storage, databases and a broad set of application services over the Internet. A cloud services platform such as Amazon owns and maintains the network-connected hardware required for these application services, while customers provision and use what they need via a web application.

AWS Global Infrastructure

AWS serves over a million active customers in more than 190 countries. AWS is steadily expanding global infrastructure to help our customers achieve lower latency and higher throughput, and to ensure that their data resides only in the AWS Region they specify. As our customers grow their businesses, AWS will continue to provide infrastructure that meets their global requirements.

The AWS Cloud infrastructure is built around AWS Regions and Availability Zones. An AWS Region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centres, each with redundant power, networking, and connectivity, housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible from a single data centre. The AWS Cloud operates 77 Availability Zones within 24 geographic Regions and two Local Zones around the world, with announced plans for 12 more Availability Zones and five more regions.

Each Amazon Region is designed to be completely isolated from the other Amazon Regions. This achieves the greatest possible fault tolerance and stability. Each Availability Zone is isolated, but the Availability Zones in a Region are connected through low-latency links. AWS provides customers with the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each AWS Region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by AWS Region). In addition to discrete uninterruptable power supply and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers.

AWS Shared Responsibility Model

Cloud security at AWS is the highest priority. AWS customers benefit from a data centre and network architecture built to meet the requirements of the most security-sensitive organisations. Security in the cloud is much like security in a customer's on-premises data centres—only without the costs of maintaining facilities and hardware. In the cloud, customers don't have to manage physical servers or storage devices. Instead, they use software-based security tools to monitor and protect the flow of information into and of out of their cloud resources.

The AWS Cloud enables a shared responsibility model. While AWS manages security of the cloud, customers are responsible for security in the cloud. This means that customers retain control of the security they choose to implement to protect their own content, platform, applications, systems, and networks no differently than they would in an on-site data centre.

The Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of the cloud security principles. AWS operates, manages, and controls the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. It is important to note that when using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

- The content that they choose to store on AWS.
- The AWS services that are used with the content.
- The country where their content is stored.
- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- How their data is encrypted and where the keys are stored.
- Who has access to their content and how those access rights are granted, managed, and revoked.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customers are responsible for the security of the content they put on AWS, or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, platforms, databases, or other services.

AWS and Customer Content

Maintaining customer trust is an ongoing commitment. AWS strives to inform customers of our privacy and data security policies, practices, and technologies we've put in place. These commitments include ownership and control of a customer's content:

a) **Access:** Customers manage access to their content and user access to AWS services and resources. AWS does not access or use customer content for any purpose without a customer's consent. AWS never uses customer content or derives information from it for marketing or advertising.

b) **Storage:** Customers choose the AWS Region(s) in which their content is stored. AWS does not move or replicate customer content outside of the customer's chosen AWS Region(s) without their consent.

c) **Security:** Customers choose how their content is secured. AWS offers strong encryption for customer content in transit and at rest, and AWS provides customers with the option to manage their own encryption keys.

d) **Disclosure of customer content:** AWS does not disclose customer content unless we're required to do so to comply with the law, or with a valid and binding order of a governmental or regulatory body. Unless we are prohibited from doing so or there is clear indication of illegal conduct in connection with the use of

Amazon products or services, Amazon notifies customers before disclosing customer content so they can seek protection from disclosure.

Security Assurance: AWS has developed a security assurance program that uses best practices for global privacy and data protection to help customers operate securely within AWS, and to make the best use of our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.