Telstra Public Submission – Security Legislation Amendment (Critical Infrastructure) Bill 2020

Telstra Executive Summary

Telstra welcomes the opportunity to provide this submission on the *Security Legislation Amendment (Critical Infrastructure) Bill 2020 Exposure Draft* (**ED**) and its accompanying explanatory document. Telstra Corporation Limited makes this submission as a participant in the Communications sector and the Data Storage or Processing sector and Telstra Energy (Generation) Pty Ltd as a participant in the Energy sector (together, **Telstra**).

We place the utmost importance on the security of our assets and infrastructure. We invest substantial resources to ensure they stand up to external and internal threats and consider all hazards in our resilience and risk planning. We welcome the Government's objective of uplifting the security and resilience of critical infrastructure through appropriate and proportional critical infrastructure reforms.

We've previously made a submission in response to the *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper* (**Consultation Paper**) in September (**September Submission**). We are pleased to see that the ED reflects some of the feedback and proposals of industry provided to date.

Our submissions on the ED can be summarised as follows:

1) **Clear co-design of sector-specific rule making**: the rules made under the proposed changes to the Security of Critical Infrastructure Act 2018 (**SOCI**) are critical to the implementation of the reforms, the critical infrastructure assets they will apply to, and the way in which the new positive security obligations will be switched "on or off". We encourage the Government to introduce a clear consultative process and timelines for the co-design of all sector-specific rules into the legislation, given the importance they play in its implementation. This should include objective criteria set out in the legislation for the making and amendment of all sector-specific rules and an ability for affected entities to seek review of the way in which the rules apply to them and the critical infrastructure assets for which they are responsible.

2) **Understanding the interaction with existing regulatory frameworks**: we recommend the Government continue to closely analyse how the reforms will interact with existing regulatory frameworks (particularly in the communications sector) and a thorough gap analysis be undertaken to provide a consistent approach to regulation. Consistent with our September Submission, Telstra's preferred approach is for Government to leverage existing obligations under the TSSR as far as possible and work closely with industry to ensure those obligations align with the new obligations under the *SOCI Act*.

3) **Clarity on application and scope of reforms:** we understand that Government has left many of the definitions for critical infrastructure assets intentionally broad with a view to providing more detail on the application of obligations in the sector-specific rules. However, we recommend that further clarity is provided in the legislation to enable businesses to have a clear understanding of the critical infrastructure assets to which the obligations apply, not only to understand their own obligations, but also those of others in their supply chain. That many of these definitions have been left to sector-specific rules further underscores the need for a clear consultative approach to the making of sector-specific rules as suggested above under section 1.

4) **Greater clarity around engagement between industry and government:** We encourage greater clarity around the terms of engagement between Government and industry to ensure the reform objectives are achieved in an appropriate and proportionate manner. We propose entities are consulted before they are issued with a notice to undertake a prescribed cyber security activity under Part 2C, and more robust protections for entities acting in good faith.

The ability for industry to recover costs from Government in limited circumstances should also be considered.

5) **Reserved exercise of Government assistance powers:** we believe that the powers of government assistance should be reserved to very limited circumstances and as a final resort. Consistent with the Consultation Paper, enlivening of these powers should be tied to a declared emergency and should be subject to review by an independent panel of experts. A legislated National Emergency Declaration (as recommended by the Bushfire Royal Commission and agreed to by the Government) would provide the necessary basis for such assistance to be given.

6) **Reconsideration of personal liability of directors:** the ED provides that where a critical infrastructure risk management program is in place, the entity must prepare annual reports on compliance that are to be signed by each individual board member. While we support the push for strong corporate governance and oversight, Telstra does not believe it is necessary for each board member to sign the report, but for the Telstra board to approve the annual report in the same way that it approves other key corporate policies and plans.

7) **Thresholds for cyber security incident reporting aligned with existing frameworks**: we recommend the threshold for reporting of 'other cyber security incidents' be set in line with the C2 level incident of the ACSC Incident Categorisation Matrix, and notification timeframes be aligned with existing frameworks such as the GDPR and CPS234.

Telstra Submission

1 Sector-specific rule making

1.1 Objective Criteria / Guiding Principles

Given the significance of the sector-specific rules, we strongly recommend that there be a clear, objective criteria or a set of guiding principles for the making and amendment of rules set out in the legislation. As it currently stands, the ED leaves much of the substantive detail around the CISONS obligations to the sector-specific rules and confers on the Minister broad powers to make and amend those rules, including the ability to 'switch on' and 'switch off' the positive security obligations for specified critical infrastructure assets.

The ED does not provide any objective criteria or guiding principles or process for the exercise of these powers. We encourage the Government to include criteria to which the Minister must have regard when making or amending sector specific rules or switching on or off particular Positive Security Obligations ('**PSOs**').

Including criteria or a set of principles will ensure that the rules are made in accordance with the objectives of the primary legislation and will provide greater certainty for responsible entities. Such an approach could be modelled on the legislative framework for the Consumer Data Right (CDR) which sets out in the *Competition and Consumer Act 2010* the criteria that the Minister must consider before designating a sector for the CDR.

In adopting this approach, Telstra would propose that the legislation require the Minister to consider, among other things, the following criteria in making or amending sector-specific rules: the likely effect on the sector as a whole, the application and scope of any obligations, the costs that are likely to be incurred by responsible entities in the sector, the interaction of existing regulatory frameworks and the need to avoid duplication of those existing regulatory frameworks, conflicts for entities operating in multiple sectors, and whether affected parties have been afforded sufficient time for proper review.

1.2 Consultation and review

Telstra welcomes the Government's commitment to consulting with industry on the making and amendment of rules and the legislative footing that this has been given at Section 30AL of the ED. We recommend that this consultation provision should not be limited to the making of rules for the purposes of critical infrastructure risk management programs, but should be extended to apply to the making and amendment of any rules, including the making of any decision to 'switch-on' or 'switch-off' PSOs for a specified class of asset. This would provide entities with surety in regard to the positive security obligation and oblige the Government to consult on the creation and amendment of all sector specific rules, not just rules relating to the critical infrastructure risk management plan.

We would recommend the Government consider introducing a clear consultative process and timeline for the co-design of sector-specific rules, and any later amendments to those rules, into the legislation similar to those which apply for the creation of sector-specific consumer data rules under the Consumer Data Right regime.[1]

We recommend that the period in which persons can make submissions should be extended from the current 14 days to 30 days to allow enough time for the preparation of considered submissions from affected parties. Further, we consider that there should be a prescribed process whereby any decision made by the Minister to make or amend sector-specific rules can be independently reviewed by an expert body (similar to the role played by the ACCC in relation to the making of consumer data rules for designated sectors).

[1] See, Divs 1 and 2, Part IVD (Consumer Data Right) of the *Competition and Consumer Act 2010*

Finally, we acknowledge that there will be circumstances in which the Minister needs to act expeditiously to amend the rules in response to an imminent threat and recognise the role that section 30AL(3) is intended to play in this regard. However, where the Minister makes or amends the rules without prior consultation under Section 30AL(3), we support the ability for entities to challenge the Ministers' actions as part of the ex-poste review process set out under 30AM. To this end, we propose that Section 30AM provide for an extended 30-day period in which parties may make submissions to the Secretary and a prescribed process for parties to seek independent review of the decision by an expert body having regard to the Secretary's statement of findings.

1.3 Application of section 30AN

Section 30AN allows the Minister to apply, adopt or incorporate a matter set out in law of a State or Territory when making rules that relate to Critical Infrastructure Risk Management Programs. This section in the ED does not make explicit reference to the application, adoption or incorporation of a Commonwealth law and raises the question of whether the Minister can refer to the TSSR when making rules that relate to Critical Infrastructure Risk Management Programs. This section, as drafted, would prevent the Minister from referring to matters in existing Commonwealth regulatory regimes, which goes against the model contemplated in the explanatory document. We recommend this section is updated to include a law of the Commonwealth.

2 Interaction with existing regulatory frameworks

The explanatory document to the ED clarifies that the new reforms will build on and not duplicate existing regulatory frameworks. We note this is not explicit in the ED. At this stage, we understand the Government's intention is to avoid duplication of existing regulatory standards or obligations (particularly in sectors with mature security frameworks such as the telecommunications sector) by using the 'switch-on/switch-off' powers available to the Minister under Part 2A while also co-designing the sector-specific rules with industry to reduce possible overlap. We understand that for telecommunications (and possibly some other parts of the communications sector) sector-specific rules will point to the TSSR obligations. However, this point is not explicit in the ED or the explanatory memorandum. Without further guidance on this issue, entities may have to apply regulatory approaches in industry-specific legislation as well as the *SOCI Act* to determine their obligations in any particular set of circumstances, leading to a higher risk of inadvertent failures to comply with one or the other as well as greater costs of compliance arising from parallel regimes. Telstra submits that the principle of "non-duplication" should be specifically reflected in the legislation through the factors that have to be considered by the Minister in the rule making process, and that where existing obligations are aligned, or made to align, the equivalent obligation under the *SOCI Act* should fall away.

As a general point, Telstra's preferred approach is for Government to strengthen existing TSSR obligations in the *Telco Act* to align those obligations with the obligations in the *SOCI Act*. To achieve this, industry should be provided with sufficient time to work with Government in mapping the obligations under each regime to ensure parity. Where existing TSSR obligations are aligned with the obligations under the *SOCI Act,* the *SOCI Act* obligations should subsequently be switched off.

Entities in multiple sectors

The explanatory document states that sector-specific rules may "deconflict requirements for entities with assets which fall within more than one definition of critical infrastructure asset",[2] however, it is not clear how this will work in practice. As previously mentioned, we recommend a more structured consultation process be adopted and the provision of clear legislative

[2] *ED294*

guidance to avoid a risk that entities who operate in multiple sectors will have inconsistent or conflicting obligations to satisfy.

2.1 Application of Part 3A

Section 35AB(d) of the ED provides that Minister's powers under Part 3A are only enlivened where "no existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a practical and effective response to the incident". The explanatory note explains that "this limb further embeds the last resort nature of this regime by ensuring it is only used when other regimes, which are potentially less invasive or which are designed specifically to address risks associated with particular assets, are not appropriate."

Telstra would welcome confirmation as to whether the Government considers the Part 3A powers to be precluded in respect of critical telecommunications assets by the Government's directions and information gathering powers set out in Divisions 5 and 6 of Part 14 of the Telco Act (TSSR).

3 Engagement between industry and government

3.1 Prior consultation

There should be prior consultation with an entity before it is issued with a notice to undertake a prescribed cyber security activity under Part 2C (e.g. cyber security exercises, vulnerability assessments, systems information reporting or systems software notices).

We suggest adopting a prior consultation model similar to that under Part 15 (Assistance and Access) of the *Telco Act* for Technical Assistance Requests (TARs). This will ensure that the powers are not exercised arbitrarily and will give entities an opportunity to make submissions on a notice before having to comply with its requirements.

This prior consultation model will be particularly important in the context of system information reporting where it will allow entities to develop clarity around – and provide feedback on – the format of the information required (e.g. raw data feeds or curated information), the methods of reporting (e.g. machine-to-machine), the regularity of reporting, and the threshold for event-based reports – all factors that will have significant cost and operational implications.

We also consider that there should be a means by which industry can voluntarily engage with government under Part 2A, reserving mandatory notices for those unwilling to undertake prescribed cyber security activities. We propose that such a model for engagement could be modelled on the graduated framework in Part 15 (Assistance and Access) of the Telco Act, which promotes and facilitates voluntary engagement, and which has been relatively successful to date.

The ability for industry to recover costs from Government should also be considered. While cyber security is everyone's responsibility, in certain circumstances – such as a national emergency – the costs of defending against a national risk, whether incurred during or because of the receipt of government assistance or otherwise, could be significant. Critical Infrastructure sectors must be able to continue to invest capital in cyber security defences and uphold and build on the security obligations, but in order to do so, it is critical that we achieve the right balance in both regulation and cost.

3.2 Protections from liability

There are several provisions in the ED that limit the liability of entities and its officers, employees and agents complying in good faith with CISONS obligations. We are of the view that some of these provisions, as drafted, do not provide sufficient protection. For example:

- There is no provision in the ED which provides that an entity is not liable to action or other proceeding for damages in relation to an act done or omitted in good faith in undertaking a cyber security exercise;

- There is no protection in the ED from liability for an entity that provides information in response to a systems information reporting notice or information gathering direction which is then misinterpreted and/or acted upon in a way that causes loss or harm;

- While annual reports (Section 30AG), evaluation reports (30CQ/30CR), vulnerability assessment reports (30CZ), systems information reports (30DH) are not admissible against an entity in civil proceedings relating to a contravention of a civil penalty provision of the Act (other than those provisions), there is nothing to prevent the reports being used in evidence in proceedings relating to penalties under other acts. There is also nothing to prevent the reports being used in evidence against officers, employees or agents.[3]

- There should also be a specific exemption for employees and agents of a responsible entity from having to give evidence in proceedings where they have assisted in the preparation of annual reports, evaluation reports, vulnerability assessments and systems information reports.

- Section 30AG provides that the annual report must be signed by each member of the board. Telstra recommends that it would be appropriate for an entity's governing body to approve the risk management plan in the same way that they would approve plans or documents relating to other significant obligations of the entity.

- Section 35AW provides an entity with protection from liability for actions undertaken in good faith in compliance with a direction given under section 35AQ (Action Direction). Similar protections are provided to an authorised agency representative where they are acting on an intervention request provided under Division 5. However, where an entity acts in good faith in response to a request from the authorised agency to undertake certain acts or provide access, the entity is not protected from any liability it may incur as a result of acting in good faith in response to such request from the agency. We recommend that the protections provided under section 35AW are extended to apply to an entity responding in good faith to an intervention request held by an authorised agency.

4 Exercise of Government assistance powers

4.1 Declared Emergency

Consistent with the Government's position in its Consultation Paper, we recommend that the ED makes it clear that there needs to be a 'declared emergency' for the Minister to authorise the Secretary to issue directions and requests under Part 3A.

To ensure there is an objective and independently verifiable basis for the exercise of government assistance powers, Telstra proposes that the Minister's powers should only be enlivened in response to an incident that has been classified as a C1 level incident under the ACSC Cyber Incident Categorisation Matrix by an independent Government agency.

4.2 Intervention requests

Telstra considers that before authorising an intervention request, the Minister should not only be satisfied that compliance with the request is technically feasible, but also that the request does not require the ASD to implement or build a systemic weakness or systemic vulnerability

[3] Similarly, Section 35AP does not prevent information being given under 35AK (information gathering direction) from being used as evidence in civil proceedings an officer, employee or agent, only the entity.

into a form of electronic protection in the system. This requirement mirrors a similar limitation set out in Part 15 (Assistance and Access) of the *Telco Act* in relation to the giving of TARs, TANs and TCNs.

Section 35AC of the ED sets out a list of certain acts that may be specified in a request to an authorised agency with a view to ensuring that interventions are appropriately targeted and reflect the specialised skills of the ASD. Some of these acts could introduce significant risks to our systems and broader eco-systems. Given the complexity of Telstra's networks, we believe that if Telstra provides the Government system information in an acceptable format to both parties, it would still allow the Government to assist Telstra in the event of a cyber incident. This would avoid risking harm or damage to Telstra's systems and reducing the risk of harm, damage or loss to data. Telstra would also be concerned with the ASD accessing its network under immunity under this regime where this previously required a warrant.

Rights of Review

Given the nature of the government assistance powers, we propose that in the absence of judicial review under the ADJR Act, there should be an alternative avenue for review of Ministerial decisions made under Part 3A, similar to that under Part 15 (Assistance and Access) of the *Telco Act* which allows recipients of a Consultation Notice for a TCN to refer the notice to an independent panel of experts for review.

5 Thresholds for cyber security incident reporting

In our September Submissions, we recommended that thresholds for mandatory incident reporting be mapped to the ACSC Cyber Incident Categorisation Matrix, with reportable incidents meeting a minimum standard of a C2 level incident.

As it is currently drafted, the threshold for reporting 'other cyber security incidents' could potentially capture a broad range of incidents. Thresholds such as 'likely' or 'imminent' threats could lead to unnecessary volumes of reporting. Telstra would welcome industry-wide consultation on the threshold for 'other' cyber security incidents, to achieve an appropriate reporting cadence that provides actionable information and insights for operators and regulators. Telstra's preference in this regard is for the threshold for reporting of 'other cyber security incidents' to be set in line with the C2 level incident of the ACSC Categorisation Matrix.

Telstra also proposes that the time frame for reporting of 'other' cyber-security incidents should be 72 hours, not 24 hours. This would align the notice period with the data breach notification periods in Prudential Standard CPS234 and GDPR.

6 Clarity on application and scope of reforms

6.1 Definitions of critical infrastructure assets

We understand that Government has left many of the definitions for critical infrastructure assets intentionally broad to capture the wide range of assets that may be considered critical to a given sector. We also understand that the Government intends to provide greater granularity around the applicability of obligations to certain particular assets through the co-design of sector-specific rules and the use of 'switch-on/switch-off' powers.

Given the Government's clear intentions in this regard, Telstra recommends that there is a clear consultative process and timeline for the co-design of sector-specific rules written into the legislation.

Providing certainty on these matters is critical for ensuring that entities understand their own obligations, and the obligations of other entities in their supply chain.

6.2 Ministerial declaration of Systems of National Significance

Consistent with our September Submission, it is our view that the nature and extent of an asset's shared interdependencies across the economy should not be sufficient in isolation to justify that an asset be a System of National Significance (**'SONS')**. Rather, interdependencies should inform how significant any impact to Australia's security, economy or sovereignty may be if the asset were compromised, disrupted or destroyed. We agree that it is relevant to consider the vulnerabilities within and between systems and networks, but the extent of this risk should be the key factor. Considering the extent of shared interdependencies alone may not appropriately capture the criticality of the asset. Consistent with the Consultation Paper, the impact to Australia's security, sovereignty and economy should be considered when assessing the national significance of a system.

Telstra welcomes the requirement at Section 52C of the ED that the Minister must consult with the relevant entity before making a declaration that an asset is a SONS. We further encourage Government to consult with responsible entities when determining whether an asset is a SONS, allowing for input prior to giving notice of a proposed declaration. We also recommend a process for review of the decision by an independent panel of experts to ensure that the designation is appropriately limited.

The fact that an asset has been declared under Section 52B to be a SONS is protected information for the purposes of the *SOCI Act*. We suggest appropriate provisions that enable a responsible entity for a SONS to disclose that to its supply chain if required to ensure that the responsible entity can comply with its obligations.