Telstra Submission – Protecting Critical Infrastructure and Systems of National Significance

Telstra Group Executive Summary

Telstra welcomes the opportunity to provide this submission on the Critical Infrastructure and Systems of National Significance Consultation Paper (**Consultation Paper**). Telstra Corporation Limited (**Telstra**) makes this submission as a participant in the Communications sector and the Data and the Cloud sector and Telstra Energy (Generation) Pty Ltd (**Telstra Energy**) as a participant in the Energy sector (together, **Telstra Group**). Telstra Health Pty Ltd as a participant in the Health sector will provide a separate submission to address the issues that apply specifically to the Health sector.

We support appropriate and proportionate critical infrastructure reforms that make our nation more secure and resilient. As identified by the Government in the 2020 Cyber Security Strategy, a close partnership between industry, Government and community is essential in driving the reform outcomes of a more secure Australia. We all have a role to play.

The Government has also recognised the need to ensure that "reforms are developed and implemented in a manner that secures appropriate outcomes without imposing unnecessary or disproportionate regulatory burden". We see this as critical in guiding participants in the next stage of consultation. Given the breadth and ambition of the reform, we are keen to support outcomes for entities operating across sectors that provide consistent and balanced regulation and compliance requirements.

In the interests of driving to the outcome of making our nation more secure and resilient, we recommend that the Government consider the different maturity levels of different sectors when determining its approach to implementation.

We recognise Government assistance can be an effective and necessary mechanism to use in an emergency situation and recommend the Government's approach to this be collaborative and reserved to limited and unique circumstances only. We encourage Government to explore a staged approach to the introduction of this aspect of the reforms.

Telstra Group has set out its submission in two parts:

- Schedule 1 outlines Telstra's comments in relation to the Communications, Data and Cloud sectors; and
- Schedule 2 outlines Telstra Energy's comments in relation to the Energy sector.

Communications, Data and Cloud Sector:

Telstra recognises that protecting its networks against all hazards is critical not only for the protection of its own customers and brand reputation but also to safeguard the broader Australian public. Telstra supports these reforms. In our submission we have made suggestions to assist in the practical implementation of the reforms. In particular, we have considered:

1) **The legislative framework**: throughout consultation, the Government has indicated its openness to suggestions from the Communications sector regarding whether the reforms would be best implemented under the *TSSR* or *SOCI Act*. After consideration of how we can assist the Government to achieve its objectives more quickly and with greater clarity, we suggest the reforms are implemented by strengthening the existing TSSR obligations.

2) **Supply chain reforms**: to ensure supply chain risks in each sector are clearly understood we suggest that during the development of sector specific guidelines, industry and Government collaborate to define and map the supply chain risks that are of greatest concern to the Government for that sector. This would avoid unnecessary cost burden by identifying the supply chains of greatest risk to critical infrastructure rather than a broad-brush approach to the use of

suppliers. We suggest this approach will also assist both the Government and each sector to understand any competitive impacts regarding the supply of foreign equipment into Australia.

3) **Implementation across sectors:** the new enhanced framework applies across multiple critical infrastructure sectors, where one entity may operate in several of those sectors. We suggest that the implementation of CI-SONS is consistent across all sectors to avoid duplication of compliance and reporting obligations to those organisations that operate in multiple sectors. We also suggest that the enhanced framework has built in protections for organisations that operate across multiple sectors to protect against liability for multiple failures triggered by one single point of failure.

4) **Criteria and final classification for 'Systems of National Significance' (SONS):** during consultation the Government identified criteria that could apply to the classification of SONS. Telstra is supportive of these criteria and has suggested that the criteria if read together would achieve a clear and appropriate threshold for entities to identify if they are operators of SONS. We would recommend that a list of SONS be agreed with the Government prior to the implementation of the reforms.

Energy Sector:

Telstra Energy is one of Australia's largest corporate consumers of energy and is also an intermediary in the National Electricity Market (**NEM**) in respect of Emerald Solar Park in Queensland and Murra Warra Wind Farm in Victoria. Telstra Energy has outlined in its submissions two key areas of focus for implementation of the reforms:

1) **mapping Regulated Critical Infrastructure Entities**: we encourage the Government to collaborate with industry in identifying Regulated Critical Infrastructure Entities. We suggest that the process to map and identify such entities should recognise that National Electricity Market registration may not always be the most appropriate point of imposing obligations and, in particular, should take into account that entities that are effectively financial intermediaries should not be identified as Regulated Critical Infrastructure Entities; and

2) **Government assistance:** we recommend that appropriate safeguards are established by the Government in relation to Government action. Consistent with our submission to the Communications, Data and Cloud sector, we recommend the Government's approach to this be collaborative and reserved to limited and unique circumstances only. In the Energy sector in particular, we encourage that the sector-specific regulations take into account the sophisticated regimes in the NEM around system security and supply. The National Electricity Law and Rules already have strict and very detailed regimes for ensuring power system security and minimising and mitigating the impacts of generators on that system. As such, the sector-specific regulations should build upon, but not duplicate or be inconsistent with, the existing energy protections in place.

Schedule 1 – Telstra Corporation Submission

Telstra has significant experience in managing large telecommunications networks and has for many years implemented a best practice security regime. Telstra also has a long and proud history of cooperating with and providing assistance to national security agencies.

As Australia's leading telecommunications and information services company, Telstra recognises the critical importance of protecting its networks against all hazards to protect its own customers and brand reputation but also for national security. Given Telstra's proven ability to manage the security and resilience of its infrastructure, and its standing as a market leader in this space, Telstra welcomes the opportunity to provide comments on the CI-SONS reforms and its likely impact on the Communications sector.

We understand the need to ensure that regulation remains relevant and appropriately adapted to cope with rapidly changing technologies and is supportive of the Government's aim to improve the management of national security risks in relation to Australia's critical infrastructure.

Given the significance, scope and complexity of the CI-SONS reforms, we would welcome the opportunity to comment on an exposure draft of the legislation. We support the Government's commitment to a phased and consultative approach to the reforms where the establishment of the principles of the enhanced framework is followed with further consultation on the sector specific guidelines.

We also consider it important that the reforms be reviewed after a period of operation to ascertain how they are operating in practice and whether the desired objectives are being achieved. Such a review should be specified in legislation from the outset so that regulated entities have clarity on the review process and period.

In order to achieve the Government's objective of improving the security and resilience of our critical infrastructure while minimising the complexity and regulatory burden of the reforms, we appreciate your invitation to comment on the proposed CI-SONS reforms.

1 Overall Framework

We support the objectives of the CI-SONS reforms and agree that a sectoral approach should be taken to implementation. We suggest the Government consider the different maturity levels of different sectors when determining its approach to implementation. Different sectors (and different participants within them) will be at different levels of maturity in terms of cyber-protection readiness. We also recommend that within a sector, the CI-SONS reforms should be designed and implemented in a competitively neutral manner.

Government will be aware that the Communications sector has been subject to existing security reporting obligations and subject to direction powers under the TSSR in the *Telco Act*, for two years now. We propose that in order to implement reforms in a competitively neutral manner, sectors that already have existing security obligations should be leveraged and utilised, rather than replaced, unless a greater efficiency can be achieved more broadly through implementing reforms under the *SOCI Act*.

The TSSR contains a security obligation with an 'all hazards' approach to security, inclusive of cyber, physical and supply chain security obligations. The security obligation is supported by a notification obligation which facilitates two-way exchange of risk mitigation information between telecommunications providers and Government; and the Government has directions powers under the regime. Further to this, we understand that the Parliamentary Joint Committee on Intelligence and Security ('**PJCIS'**) has commenced its statutory review of the TSSR, which we anticipate will enhance and focus on improving how this regime operates to meet the security objectives of the Government.

We support the proposed iterative approach to develop the reforms. As the sector specific standards will require more detailed co-design and therefore require more time to develop, we agree that development

of these standards should commence in parallel with the sector-agnostic principles and take effect once the sector agnostic principles have been agreed.

We encourage the Government to work in parallel to ensure that government panels and contracts are consistent with the CI-SONS reforms. Given that the CI-SONS reforms will require entities to uplift security requirements to a requisite level, this should also be sufficient to satisfy Government's contractual expectations in areas of overlap.

We commend the sectoral approach set out in the Consultation Paper, but prior to the implementation of sectors, we suggest that the Government and industry collaborate to agree an approach that supports entities that operate in multiple sectors. We would recommend that an approach allows entities operating in multiple sectors to comply with the Positive Security Obligation (**'PSO'**) on a consistent and where appropriate, aggregated, basis to reduce duplication of effort and avoid conflicting and inconsistent regulation, regulatory approaches and requirements (particularly if there are different regulators that take different approaches to compliance within their sectors). This should avoid different sectors having substantially similar obligations that are expressed slightly differently, or with slightly different compliance and reporting regimes. To the extent that this does occur, we recommend compliance with the obligations imposed on a primary sector should be deemed compliance with the requirements of other sectors.

A sector overlap issue that is particularly relevant to the Communications sector is the Data and the Cloud sector. Many of our data and cloud services are embedded in or provided in connection with other managed services we provide to customers or receive from suppliers.

Consistent with our recommendation above, we think that for entities that participate in both the Communications sector and the Data and Cloud sector, there should be a provision that effectively only requires compliance with the one instrument (i.e. the Communications sector specific guidelines). This could be done explicitly, or through a deeming approach, which deems an entity to have complied with the requirements in relation to the Data and Cloud sector if it has complied with the obligations imposed on the Communications Sector. Such an approach is consistent with the proposed approach for communications related space assets.

Finally, where single entities are participants in multiple sectors we encourage the Government to consider adopting appropriate protections to ensure that a single perceived or actual failure to comply with the obligations is not considered to be a separate failure in each sector.

We look forward to continuing to work with the Government to shape an approach to implementation during the next phase of the consultation process.

1.1 Building upon existing regulatory frameworks

The Consultation Paper clarifies that the new reforms will build on and not duplicate existing regulatory frameworks. The Government has also called for views from the Communications sector during consultation in relation to whether the reforms would be best implemented under the *TSSR* or *SOCI Act*.

We have considered this request and suggest the PSO and any further enhanced security obligations and assistance in the Communications sector could be most efficiently implemented through amendments to the *Telco Act,* for the following reasons:

- The *Telco Act* includes security requirements introduced as part of the TSSR in 2018. It also includes other telecommunications sector-specific legislative instruments that appropriately cover security and an all-hazards approach. This includes, for example, protection of communications in Part 13, national interest matters in Part 14, industry assistance in Part 15 and defence requirements and disaster plans in Part 16 of the *Telco Act*, carrier licence conditions and service provider rules, which could all be used to implement the Government's CI-SONS reform objectives. We encourage the Government to consider these obligations in aggregate when considering whether it would be more efficient to implement the reforms under the *Telco Act*.

- While the proposed CI-SONS reforms would build on and will provide more specificity than the TSSR's existing obligations, we believe strengthening the existing TSSR obligations will achieve the Government's objectives for the Communications sector and at the same time allow the Government to focus on sectors that require the greatest uplift.

- The TSSR also provides the Government with directions powers and carriers and carriage service providers are required to notify and share information with the Government in relation to changes that may impact the security of their networks.

- As the TSSR was implemented in 2018, carriers and carriage service providers have developed practices to manage requirements under the *Telco Act* and can more easily build from that known base rather than starting anew under a different framework. Similarly, the Critical Infrastructure Centre has developed processes and recently updated guidelines which can be leveraged to achieve the Government's policy objective.

- The *Telco Act* framework leverages appropriate governmental expertise. We consider that the Australian Communications and Media Authority (**ACMA**) and the Critical Information Centre ought to continue to exercise their respective functions to monitor and enforce security obligations of the Communications sector.

We anticipate that there will be some obligations under the *Telco Act* that will overlap with obligations proposed by the CI-SONS reforms, particularly if captured under the *SOCI Act*, because the corresponding rights offered under the *Telco Act* are not offered under the *SOCI Act*. An example of this is in relation to threat sharing, currently this can be done under varying provisions under the *Telco Act*, including a s 313(3) request, a TAR, or through voluntary disclosure provisions. These requests will not be available under the *SOCI Act* and we suggest that further consultation and design will be required to develop how these obligations could sit together or be removed (which may have carry on effects to law enforcement regimes). The result is that reforms could be advanced more rapidly and with greater clarity by building upon the *Telco Act*.

If the Government considers a single instrument is preferable, we suggest the *SOCI Act* and *Telco* Act requirements co-exist with appropriate deeming provisions and strengthened provisions in the *Telco Act* to address any gaps. In other words, carriers and carriage service providers should be deemed to have complied with the requirements of the *SOCI Act* to the extent that they have complied with corresponding obligations under the *Telco Act.* For example, compliance with the PSO under the *SOCI Act* can be deemed to be satisfied through entities' compliance with the TSSR (to the extent uplifted to address any necessary gaps).

This will have the benefit of ensuring key requirements regarding critical infrastructure are dealt with in the one place (i.e. under the *SOCI Act*), but do not change processes which are working well under existing frameworks. Under this model, a participant in the Communications sector should not be in breach of both the *Telco Act* and the *SOCI Act* for a single failure to comply with an obligation.

1.2 Ownership and control

We understand that the new reforms will extend existing ownership and control reporting requirements under the *SOCI Act* to new sectors.

Under the Communications sector, Carriers are required to provide detailed information about organisational structure, foreign ownership and the network and technology used to supply carriage services as part of the carrier licensing requirements.

We are keen to explore how this information could be leveraged to avoid duplication.

1.3 Entities covered by the enhanced framework

We consider the Enhanced Cyber Security Obligation, which will apply only to SONS, should be technology focussed and linked to the relevant critical system or infrastructure. This is particularly important where entities own or operate multiple different infrastructure assets that may fall into different categories.

As identified in the Consultation Paper, we understand that Government will consult with industry to map and identify what should become a Critical Infrastructure Entity, a Regulated Critical Infrastructure Entity and assets that will be designated as SONS. To do this, the regime contemplates mapping interdependence with other functions. This is likely to be a significant task for all sectors and we encourage Government to provide appropriate parameters around how this activity will be coordinated.

(a) Critical Infrastructure Entities

We consider that it would assist participants if the proposed approach to the definition of critical infrastructure assets is more precise. The current definition proposed by the Department of Home Affairs in Communications Workshop held on 1 September 2020 suggests that assets, systems or networks associated with the delivery of services by industries involved in the provision of postal, electronic and other communications will be critical infrastructure assets. This definition is broad and could capture most entities in the Communications sector. We recommend that the definition is more clearly defined and a relevant threshold applied so that entities are able to operationalise the reforms.

(b) Regulated Critical Infrastructure Entities

We support the Government's proposal that carriers and carriage service providers, as defined under the *Telco Act*, be identified as Regulated Critical Infrastructure Entities.

(c) SONS

Our understanding from details circulated after the Communications Workshop held on 1 September 2020 is that SONS will include assets that the Minister considers are assets of national significance. This view will be informed by an assessment of:

a) the impact to Australia's security, economy or sovereignty should the asset be compromised, disrupted or destroyed;
b) the extent of shared interdependencies of the asset across the economy; and
c) any other matters the Minister (for Home Affairs or as appropriate) considers relevant.

We recommend that the final classification be sufficiently clear to ensure that all entities understand whether they own or operate a SONS. Uncertain criteria may result in confusion and increased compliance costs.

We recommend in particular that items a) and b) above be considered together as one threshold. The extent of an asset's shared interdependencies across the economy should not be sufficient in isolation to justify that an asset be a 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.

In addition, a materiality level should apply to the threshold. The impact to Australia's security, economy or sovereignty of a compromised, disrupted or destroyed asset should be *catastrophic* in order for the Minister to be satisfied that an asset is a SONS. A materiality requirement is necessary to ensure that only the most important and critical assets are classified as SONS.

We consider that only a very limited number of Telstra's assets or systems would be regarded as a SONS. Telstra will provide a specific list of such assets or systems at the appropriate time.

1.4 Call for views

Our response to the specific "call for views" made by Government are set out below.

#	Question	Telstra Response
1	Do the sectors above[1] capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?	We recommend considering changing the Transport sector title to "Transport and Logistics". Logistics companies that supply critical freight operations should be considered Critical Infrastructure, similar to the approach taken in the United States by the Cybersecurity and Infrastructure Security Agency. Government should be a cyber security exemplar to industry by strengthening the defences of its own systems. Government systems that perform critical functions or contain sensitive information i.e. Australian Electoral Commission (AEC) systems, ATO, Services Australia, My Health Record, MyGov etc should also be designated as SONS. Manufacturers of physical technology assets for the Communications sector, such as fibre and other network infrastructure and hardware remain vital elements of Telstra's network and should also be subject to the reforms. This will assist in limiting supply chain risk and removing the requirement to negotiate compliance with security obligations through contract.
2	Do you think current definition of Critical Infrastructure is still fit for purpose?	We consider that it would assist participants if the proposed approach to the definition of critical infrastructure assets is more precise. The current definition proposed by the Department of Home Affairs in Communications Workshop held on 1 September 2020 suggests that assets, systems or networks associated with the delivery of services by industries involved in the provision of postal, electronic and other communications will be critical infrastructure assets. This definition is broad and could capture most entities in the Communications sector. We recommend that the definition is more clearly defined and a relevant threshold applied so that entities are able to operationalise the reforms.
3	Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?	As indicated above in response to question 1, the effectiveness of many of the sectors are underpinned by the availability and effectiveness of manufacturing and logistics providers. These additional sectors should be made subject to the reforms to avoid supply chain risks. A compromise to either of these industries could significantly impact the ability of energy, water, communications, food and groceries and banking to provide services, which could consequently cause a significant impact to the social or economic wellbeing of the nation or to ensure national security.
4	What are the common threats you routinely prepare for and those you have faced/experienced as a business?	Telstra's approach to cross company resilience is to prevent, detect, plan, withstand and subsequently recover from the impacts of disruptive events. This resilience approach is achieved through a number of key elements: • **Cross Company Resilience Framework** • **Business Resilience** – takes an all hazards approach to continuity planning for recovery of Telstra critical business processes

[1] • Banking and finance • Communications • Data and the Cloud • Defence industry • Education, research and innovation • Energy • Food and grocery • Health • Space • Transport • Water

#	Question	Telstra Response
		• **Technology Resilience** – takes an all hazards approach to Information Technology Disaster Recovery Planning for recovery of critical business applications and associated systems; • **Network Resilience** – built in Network Resiliency with Redundancy and Network Monitoring for prompt attention for potential disruptions • **Cybersecurity** – robust cybersecurity risk management underpinned by effective cybersecurity practices and controls. • **Supplier Resilience** – we require our suppliers to have appropriate and effective controls in place to ensure provision of contracted goods and services to Telstra. • **Incident Management** – we take a proactive approach to effectively manage and resolve the cause of disruptive events and return to normal business operations as quickly as possible. • **Crisis Management** – this is the highest level of response and management, which is invoked for the most severe or damaging events. • **Emergency Management** – we have detailed plans and processes in place to support Emergency Services Organisations during emergency situations.
5	How should criticality be assessed to ensure the most important entities are covered by the framework?	Criticality of an asset should be assessed by the impact or consequence of a failure of the asset to Australia's economy, national security and sovereignty and the interdependency of that asset on other critical assets that service the Australian economy, public or security of the nation. SONS should relate to the specific "technology and systems" that if compromised would have a catastrophic impact on the economy, safety or national security of the nation. Interdependencies should be considered as part of this assessment and not separately.
6	Which entities would you expect to be owners and operators of systems of national significance?	Our understanding is that SONS will include assets that the Minister considers are assets of national significance and that this view will be informed by an assessment of: a) the impact to Australia's security, economy or sovereignty should the asset be compromised, disrupted or destroyed; b) the extent of shared interdependencies of the asset across the economy; and c) any other matters the Minister (for Home Affairs or as appropriate) considers relevant. We consider that, with the application of appropriate materiality thresholds applied to the above criteria only a very limited number of assets or systems would be regarded as a SONS.

2 Government - Critical Infrastructure Collaboration to Support Uplift

We welcome the acknowledgement of the importance of ongoing collaboration between industry and Government reflected in the Consultation Paper. We encourage Government and regulators to embrace cross-sector engagement to ensure strategic alignment of requirements given the interconnectedness of our critical infrastructure systems.

We recommend that compliance requirements, awareness and educational programs be tailored to different infrastructure owners and operators based upon their size, sophistication, the nature of the infrastructure for which they are responsible and the risks they face. It is important that the CI-SONS reforms are implemented in a way that does not create conditions which impact the competitive position of entities within each sector. We also consider that wherever possible, maturity frameworks should be used so that infrastructure owners and operators improve their cyber security defences over an appropriate length of time.

We support the development of a revised Trusted Sharing Network for Critical Infrastructure and Critical Infrastructure Resilience Strategy and provide our insights on the initiatives below.

2.1 Call for views

Our response to the specific "call for views" made by Government are set out below.

#	Question	Telstra Response
7	How do you think a revised Trusted Information Sharing Network for Critical Infrastructure (**TISN**) and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?	A revised and likely expanded TISN will be most useful for its cross-sector and intra-sector convening power, particularly when it comes to mapping interdependencies for the Positive Security Obligation. It should also be leveraged to disseminate all-hazards information across relevant sectors. However, for the Enhanced Cyber Security Obligation, the Australian Cyber Security Centre's network of partners under the Joint Cyber Security Centre programme and the National Information Exchange communities, is best placed for sharing cyber security technical and operational best practice and threat information. Any attempt to specialise the TISN into cyber security would risk duplicating these existing mechanisms.
8	What might this new TISN model look like, and what entities should be included?	All sectors included under the reforms should be included in the new TISN model. TISN should perform a strategic coordination role that does not overlap with existing mechanisms and bodies e.g. ACSC/JCSC, NIE and CISOLens, to reduce duplication and resource burden. The TISN could be used as a central forum to set thresholds and expectations for communications and actions in a cyber incident, both between industry and government, and within/across sectors. A revised Critical Infrastructure Resilience Strategy could set out the thresholds and expectations for declaring a cyber emergency and resultant actions. This should link into the Cyber Incident Management Arrangements which are managed by Home Affairs and leverage the Cyber Incident Categorisation Matrix that currently sits with the ACSC. TISN could also be the focal point for incident readiness / "preparatory" activities. It is ideally placed to model and test cross-sector dependencies in an incident, drawing in relevant all-hazards expertise from various organisations.

#	Question	Telstra Response
9	How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?	• Identify and share with industry cross sector dependencies to assist sectors to identify and protect against otherwise unknown risks. • Facilitate the development of cross-sector enhanced frameworks and policies. • Provide targeted cross-sector threat assessments and briefings. • Quickly disseminate alerts to all directly or indirectly impacted parties on critical issues and details of compromises impacting both critical entities but also their supply chains. This process could leverage security-cleared staff in the private sector, if required. This knowledge allows entities to better assess their potential exposure.

3 Initiative 1 – Positive Security Obligation and Reporting

We support the establishment of minimum cyber security requirements and are pleased that the Government has sought input from industry on the specific requirements.

With regard to the proposed mandatory incident reporting requirement, we suggest that industry and Government agree the scope and breadth of this requirement during co-design of sector-specific standards in order to ensure it does not impose unnecessary operational costs on businesses, particularly businesses with regulated pricing and SMEs. In order to mitigate the burden on both infrastructure operators and security agencies, we suggest thresholds for notification of an incident are set and meet the minimum threshold of a C2 incident under the national Cyber Incident Categorisation Matrix. We also recommend that reporting avoids unnecessary disclosure of personal information, internal security and commercially sensitive information.

3.1 Principles-based outcomes and security obligations

We recommend that sector specific standards be implemented by the industry regulator. Within each sector, the regulator will need to ensure the consistent application of regulations to ensure certainty and competitive neutrality within the sector. For example, different participants in a sector should not be held to different standards merely because of differences in organisational capability or the level of resource they decide to apply to complying with the PSOs.

As discussed in Part 1.1, we consider that the *Telco Act* already provides a very strong basis for specific standards appropriate for the Communications sector.

3.2 Supply chain security

We support an “all hazards” approach to security. Under the TSSR, we are required to demonstrate competent supervision and effective control over our suppliers.

We recommend that prior to the development of sector specific guidelines, industry and Government should collaborate to define the critical security risks to supply chain and implement guidelines as to how supply chain security should be implemented. This could include providing templates and pro forma standards or questions which will ensure consistency in how entities set expectations in their supply chain. We believe this will benefit smaller entities down the supply chain who can adopt practices and responses which will meet the standardised requirements of their customers.

At the same time as mapping the supply chain risks, the competitive impact to industry, if Government becomes too prescriptive in relation to which suppliers an entity may or may not use in Australia, should be addressed, particularly in relation to the provision of equipment.

3.3 Reporting to regulators

We suggest that the reporting obligations should not require unnecessary disclosure of internal security and commercially sensitive information. The scope and breadth of reporting could have significant operational costs on businesses and should be subject to appropriate thresholds to mitigate this risk.

We consider that the thresholds applied to notifications required by the TSSR under the *Telco Act* are appropriate. Carriers and carriage service providers have an obligation to notify of proposed changes to a telecommunications service or a telecommunications system that are likely to have a material adverse effect on their capacity to do their best to protect telecommunications networks and facilities from unauthorised interference or access. Examples of such changes include providing new telecommunications services and changing the location of telecommunications equipment. The benefit of this approach is that the TSSR facilitates a foundation for compliance and requires reporting where there is a deviation to this foundation.

We are particularly interested in working with Government regarding the proposed mandatory incident reporting requirement. We acknowledge that incident reporting in this context differs from the TSSR notification obligation and the customer data breach notifications required by the OAIC. This may impose a significant reporting burden. We suggest that clear thresholds are agreed between Government and industry, to protect against the ambiguity and cost of compliance. Mandatory reporting should only be for the most serious incidents and voluntary cooperation and threat sharing should be encouraged for less

serious incidents. It is important that the appropriate balance is reached between mandatory reporting and voluntary cooperation.

We recommend that thresholds for mandatory incident reporting be mapped to the ACSC Cyber Incident Categorisation Matrix. Reportable incidents should meet a minimum standard of a C2 level incident. C2 level incidents relate to the sustained disruption of essential systems and associated services, exfiltration or deletion/damage of key sensitive data or intellectual property within essential services and critical national infrastructure. This threshold ensures that the most serious incidents are reported to government, removing the "noisy" and less serious incidents which can adequately be handled by internal security teams.

3.4 Call for views

Our response to the specific "call for views" made by Government are set out below.

#	Question	Telstra Response
10	Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?	The principles-based outcomes appear to be sufficiently broad to capture all aspects of security risk, and to endure as technology evolves and develops. TSSR is also an all-hazards approach and could easily be amended to provide the additional compliance framework desired under the proposed reforms. The TSSR has been in place for two years and telecommunications providers have settled into a good operating rhythm with the Critical Infrastructure Centre. To change this now, when the TSSR already sufficiently covers the PSO and can be further enhanced to include additional reporting requirements, would create an additional unnecessary regulatory burden on carriers and carriage service providers.
11	Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?	Effective and diligent co-design with industry of the sector-specific guidelines will be critical to define clear expectations in relation to the security requirements. We consider that the scope and breadth of mandatory incident reporting could have significant operational costs on businesses. In order to mitigate the burden on both infrastructure operators and security agencies, thresholds for notification should be set very clearly and be mapped to the ACSC Cyber Incident Categorisation Matrix. Notifications should meet the "C2" incident level at a minimum. The reporting should also avoid the unnecessary disclosure of internal security and commercially sensitive information. These will need to be established in the co-design of sector-specific standards.
12	Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?	Telstra is already operating in-line with the security principles under the TSSR. Uplifting the TSSR obligations to align with the PSO obligations, rather than incorporating the reforms under the *SOCI Act* will help to mitigate some costs that may arise in relation to the new reforms.
13	What costs would organisations take on to meet these new obligations?	There will be additional processes and resources required to ensure that the reporting requirements can be met by the new reforms. However, we anticipate there is scope for these costs to increase as a result of an increased number of requests for mandatory threat sharing. The number of reports per year and the relevant threshold for reporting will also impact the cost to organisations to comply with these obligations.

#	Question	Telstra Response
		We anticipate the reporting obligations and regulated threat sharing will impose additional costs.
14	Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?	The telecommunications and banking sectors are both subject to a security obligation in line with these principles, TSSR and CPS234. The obligations under the TSSR take an all-hazards approach to security covering cyber, physical, personnel and supply chain security. The TSSR obligation would require enhancements to cover additional reporting requirements anticipated by the CI-SONS reforms, however without a detailed understanding of the scope of additional reporting anticipated by the reforms or any information regarding sector-specific requirements, it is not currently possible to anticipate the costs associated with the uplift.
15	Would the proposed regulatory model avoid duplication with existing oversight requirements?	The telecommunications sector already has a security obligation, which takes an all-hazards approach to security and covers cyber, physical, personnel and supply chain security. It is expected that the PSO will be more prescriptive than the TSSR in relation to how an entity is to comply and report. As noted above, we consider that additional elements could be captured via an enhanced TSSR obligation to avoid duplication. Also, the Government has just released a revised version of the administrative guidelines for the TSSR. To avoid duplication, it would be beneficial for these guidelines to be utilised for any enhancement of the PSO captured under the *Telco Act*. We also note that the PJCIS has just recently commenced its review of the TSSR, any recommendations from that review should be leveraged.
16	The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?	Refer to the response above regarding the administrative guidelines. In addition to this, we recommend that the sector specific guidelines include detail on thresholds for reporting, example best practice in how to meet the obligation, clear categorisation of what is in scope and case studies/scenarios to support clarity. Regular e.g. monthly sector working groups for Q&A should also be held to share experiences/case studies and clarify implementation issues.
17	Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?	For telecommunications, the Critical Infrastructure Centre undertakes the regulatory role. This model is working well under TSSR and we have co-developed an effective engagement model over time. For the Communications sector it is recommended that the Government build on this model to add in any additional obligations in close consultation with the Critical Infrastructure Centre.
18	What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?	We suggest the following: • Training / uplift in understanding “all-hazards” and cyber risk.
19	How can Government better support critical infrastructure in managing their security risks?	• Regular threat briefings, relevant information sharing. • Clear, concise, timely, scenario-specific advice that is easy to share with relevant specialist teams e.g. networks, procurement, finance.

#	Question	Telstra Response
		• Focus should be on less mature sectors to achieve desired uplift promptly.
20	In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?	Telstra routinely conducts background checks when appointing people as employees or engaging them as contractors using a risk-based approach. The background checks undertaken depend on the nature of the role and responsibilities the employee/contractor will undertake and which information, customers and systems they will have access to. We do not believe there is currently a need to introduce AusCheck as an additional assessment over and above Telstra's existing due diligence.
21	Do you have any other comments you would like to make regarding the PSO?	The Consultation Paper does not provide detailed guidance with respect to physical security expectations. As Telstra already has a mature and advanced framework for all-hazards security as a result of the TSSR, we would argue that further uplift in relation to this obligation should be related solely to enhanced reporting, but not further enhanced standards.

4 Initiative 2 – Enhanced Cyber Security Obligations

Telstra recognises the importance of threat sharing in protecting the country's critical infrastructure and nation. This is a view held by much of industry which already shares threat information with Government voluntarily. Industry and Government will need to work together to ensure that regulation of this voluntary relationship does not impact the quality of the information shared.

There is a common interest between industry and Government in assuring the security of important infrastructure assets. As such, we recommend an approach that is flexible, cooperative and collaborative. This is more likely to promote constructive behaviour than initiatives that are rigid and subject to punitive fines or other regulatory consequences.

4.1 Situational awareness

Telstra maintains a well-developed threat-sharing relationship with the Government and we are committed to maintaining this positive and trusting relationship.

We consider that further clarity is required regarding the "network and systems information" gathering activities proposed. This is currently a broad term that could encompass commercially and customer sensitive information. The scope of what this information includes must be agreed in sector specific guidelines and should only at most relate to information concerning designated SONS. Further clarity is required regarding whether the information will only be shared with Government, or whether it will be shared across sectors. If information is shared to industry more broadly, this may create competition and confidentiality issues for entities.

We also consider that any mandatory situational awareness sharing should only apply to infrastructure that connects or is located in Australia. Mandatory information sharing should not extend to information that an entity is legally obliged to protect or not disclose and should include safeguards in relation to ensuring the confidentiality and control of the information. We recommend that preparatory activities should be light touch, voluntary and conducted in partnership with the entity concerned.

We are supportive of the Government's commitment to whole-of-economy cyber security exercises and playbook creation. We encourage the inclusion of oversight requirements and clarification on whether the activities will be mandatory or cooperative.

4.2 Call for views

Our response to the specific "call for views" made by Government are set out below.

#	Question	Telstra Response
22	Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?	We don't believe there are additional activities required.
23	What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?	Contextualised, accurate, relevant, and timely threat information that is complete.
24	What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?	Telstra welcomes the opportunity to discuss this further with the Government.
25	What methods should be involved to identify vulnerabilities at the perimeter of critical networks?	Mature cyber organisations scan their internet-facing infrastructure as a component of good vulnerability management.
26	What are the barriers to owners and operators acting on information alerts from Government?	To assist owners and operators, alerts could be enhanced by the provision of key details, including timelines for observed activity or contextual information.
27	What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?	It would be helpful if Government and industry could co-design a template for the playbooks. Barriers include Government committing skilled resources to facilitating and co-ordinating national exercises. Key details to include clarification of incident thresholds and expectations, and communications processes e.g. how communications flow, are approved and at what level. Learnings from exercises should be built into key policy frameworks, such as the Cyber Incident Management Arrangements.
28	What safeguards or assurances would you expect to see for information provided to Government?	Maintain confidentiality of the information provided, respect handling/distribution limitations placed on the information shared and protection for entities against liability for any action taken on the basis of information shared. Information must only be shared across a secure system, exclude any customer information or commercial information of Telstra. The Government must agree with each entity who will receive the information, including which agencies within Government will receive such information and then how that information will be used by those agencies.

#	Question	Telstra Response
		Sharing of information will remain subject to any existing legal obligations in relation to the disclosure of Telco Data.

5 Initiative 3 – Cyber Assistance for Entities

We believe that intervention by the Government should be collaborative, reserved to very limited and unique circumstances and as a final resort.

5.1 Safeguards

We suggest appropriate protections for (a) information that may be accessed as a result of the Government assistance powers and (b) any contractual liabilities or consequences arising as a result of Government assistance. This should include clear limits and a legal framework that sets out when and for how long the Government can provide assistance to an entity. This framework should also embed consultation as part of the required process.

To support independence in Government and appropriate use of powers we recommend that any intervention be based on advice by independent Government agencies responsible for national security (as is the case under the TSSR, for example). Government assistance and/or a reasonable and proportionate direction should not be issued until an adverse security assessment has been provided.

We recommend, similar to the TSSR, that decisions are subject to review under the *Administrative Decisions (Judicial Review) Act 1977* (Cth), to ensure there are adequate checks and balances in place to review decisions made by the Government in these circumstances. In addition, infrastructure operators should have immunity from any liability arising from actions taken in accordance with Government directions or otherwise arising from Government intervention, including for contractual liability to suppliers and customers affected.

Cost recovery should also be available for entities in certain circumstances, particularly where costs are incurred (for e.g. as a result of damage to property or systems) due to Government intervention. We consider it important that the reforms preserve the principle of cost recovery which is well established under the *Telco Act*, for example, where carriers and carriage service providers provide help under s 313 of the *Telco Act*.

5.2 Entity and government action

Subject to appropriate protections, we agree that Government should have the power to issue reasonable and proportionate directions to entities to ensure that action is taken to minimise the impact of imminent cyber threats or incidents.

Clear thresholds should apply to the Government's power to issue a direction. In addition to the safeguards outlined in section 5.1 a reasonable and proportionate direction should not be given unless:

- it is reasonably necessary for the purpose of national security;
- the entity is capable of complying (and there should be a defence for the entity to the extent that it is not legally or technically capable of reasonably complying with the direction);
- reasonable steps have been taken to negotiate in good faith with the entity to achieve an outcome without a direction being given; and
- no existing regulatory system of the Commonwealth, a State or a Territory could instead be used to eliminate or reduce the risk that is sought to be addressed by the direction.

We are of the view that even under an emergency declaration, the Government's approach to assistance should be collaborative and reserved to limited and unique circumstances. We also recommend that the Government take reasonable steps to negotiate with the entity a time limit on its use of the power to take direct action and that exercise of this power be subject to independent authorisation.

5.3 Call for views

Our response to the specific "call for views" made by Government are set out below.

#	Question	Telstra Response
29	In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?	Consideration of an entity's security maturity and demonstrated historical collaboration with Government on security, should be assessed prior to determining whether Government assistance is necessary or not. We recommend the Government's approach to this be collaborative and reserved to limited and unique circumstances only.
30	Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?	The Prime Minister upon consultation and advice from the Minister for Home Affairs based on the declaration of a cyber crisis by the ACSC or an ASIO Adverse Security Assessment.
31	Who should oversee the Government's use of these powers?	We believe Government assistance powers should be subject to review under the *Administrative Decisions (Judicial Review) Act 1977* to ensure there are adequate checks and balances in place to review decisions made by the Government in these circumstances. We recommend that the Government's use of these powers be based on advice by independent Government agencies responsible for national security (as is the case under the TSSR, for example).
32	If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?	We believe this is a matter for Government.
33	What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?	Where Government exercises a direction power or provides assistance to entities affected by an attack, both Government and the entity should be entitled to immunity from claims from or losses suffered by third parties in connection with the actions taken by or at the direction of Government. This should include immunity to the extent that the entity undertakes or is required to undertake an act that would otherwise cause it to breach a law of the Commonwealth or a State/Territory.
34	What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?	• Government assistance decisions should be subject to review under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) to ensure there are adequate checks and balances in place to review decisions made by the Government in these circumstances. • A reasonable and proportionate direction should not be issued until an ASIO Adverse Security Assessment has been provided. • Immunity should be afforded to entities that have been required to take action either on direction by the Government or liability arising as a result of Government action (refer to answer under question 33). • Clear limits and a legal framework will need to be introduced to set out when, for how long and to what extent Government should and could provide assistance to an entity (refer to our response to question 29 regarding whether this power should

#	Question	Telstra Response
		apply to entities with a mature security posture that already comply with similar security obligations).
35	What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?	There is risk that Government direction or Government action creates unintended consequences that could exacerbate the cause or prolong a network outage. In cases where the affected entity has a mature security framework, the operator of the network is likely to be best placed to take measures to protect the network. Industry participants should be indemnified against adverse effects of following Government direction and against adverse effects of Government action.
36	Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?	Government should only intervene in exceptional circumstances. The approach should not be informed by the view that Government is better placed to take action, but rather from the perspective that Government is required due to the failure of an entity to take such action.

Schedule 3 – Telstra Energy Submission

Telstra Energy (Generation) Pty Ltd (**Telstra Energy**) is an active participant in the National Electricity Market (**NEM**) as one of Australia's largest corporate consumers of energy and through its infrastructure which includes backup generators and batteries, participates in the wholesale electricity market. Telstra Energy is also an intermediary in the NEM in respect of Emerald Solar Park in Queensland and Murra Warra Wind Farm in Victoria. As part of the contracts entered into with the project owners to develop these projects, Telstra Energy is registered as a generator with the Australian Energy Market Operator (**AEMO**) instead of the project owners and receives the wholesale market revenue directly from AEMO but does not have physical possession of the projects or control over the operation or performance of the projects.

Telstra Energy's role and responsibilities in relation to these assets exemplifies why not all entities engaged in the activity of owning, controlling or operating a generating/storage system should be responsible for complying with the PSO. The responsibility of primarily financial intermediary entities, such as Telstra Energy, under the CI-SONS reforms should be limited to complying with Government assistance where appropriate.

Telstra Energy limits comments on the Consultation Paper to the following:

1) **Regulated Critical Infrastructure Entities:** The Government's approach to identifying and mapping Regulated Critical Infrastructure Entities is significant as those entities will be required to comply with the PSO. In the Energy Sector, there are often multiple entities involved in an asset who have differing roles and responsibilities. We consider that the approach outlined in the Energy Sector Workshop on 27 August 2020 is too broad as it may result in entities being identified as Regulated Critical Infrastructure Entities which are not, and should not, be in a position to comply with the PSO. NEM registration may not always be the most appropriate point of imposing obligations and, in particular, entities who are effectively financial intermediaries should not be identified as Regulated Critical Infrastructure Entities.

2) **Government intervention**: Telstra Energy shares the views and recommendations made by Telstra Corporation in Schedule 1 regarding proposed powers of the Government to issue reasonable and proportionate directions and take direct action. Further, sector-specific reforms must take into account the existing sophisticated regimes in the Energy sector. Directions should only be made to entities that are capable of complying with that direction. Further, there should be a defence available for entities that do not comply with a direction to the extent that they are not legally or technically capable of reasonably complying with the direction.

1 Regulated Critical Infrastructure Entities

Telstra Energy recommends that the scope of entities deemed to be Regulated Critical Infrastructure Entities be clarified. A clear scope is important in ensuring that the PSO applies to entities that are best placed to meet the requirements and ensure security of the asset. If only one Regulated Critical Infrastructure Entity is to be appointed for an asset, then the entity registered in the NEM may not be appropriate person as they will not always be the person who is best able comply with the PSO. If numerous Regulated Critical Infrastructure Entities are to be appointed in relation to one asset, this may create confusion regarding individual responsibilities and will be problematic with common ownership and operating structures used in the NEM if entities with little control will be required to comply with the PSO.

At the Energy Sector Workshop held on 27 August 2020, it was proposed that Regulated Critical Infrastructure Entities in the Electricity sector would cover:

1) Electricity generation and storage:

    - Any person who engages in the activity of owning, controlling, or operating a generating/storage system directly connected to an electricity network or electricity system with a total nameplate rating of more than 30 MW in the NEM, 10 MW in the WEM, NWIS and NT

    - Energy systems that provide system restart ancillary service

2) Electricity transmission and distribution

    - A network, system, or interconnector, for the transmission/distribution of electricity to ultimately service at least 100,000 customers

3) Market operators

    - Electricity or gas market operation

Such entities will be required to comply with the PSO. This involves a responsibility to take an all-hazards approach when identifying and understanding risks. It requires consideration of natural and human induced hazards and includes understanding how these risks might accumulate throughout the supply chain. The PSO would also introduce new requirements for board accountability concerning cyber security.

Telstra Energy considers that the proposed approach is not appropriately targeted and will result in entities that are not positioned to comply with the PSO being caught by the regime in circumstances where it is more appropriate for another entity to meet the obligation and ensure security of the asset. A clear example of this is where an intermediary has been appointed for a generator.

In the NEM, only one person can be registered with AEMO as a generator. Where more than one entity owns, operates or controls the generator, one entity registers with AEMO as an intermediary and the others are exempted from registration. It is quite common for generator projects to have intermediaries.

In Telstra Energy's case, it entered into power purchase agreements with Emerald and Murra Warra to underwrite the construction of those projects. Under the agreements, Telstra Energy registered as intermediary for the project and the project owners are exempted. Telstra Energy is responsible for bidding the generators into the NEM, has some limited dispatch control for pricing purposes and receives the wholesale market revenue directly from AEMO. However, Telstra Energy does not have physical possession or control of the plant, does not control its operational systems and is not responsible for its maintenance.

In terms of the PSO principles-based outcomes, "financial" intermediaries such as Telstra Energy are not in a position to:

1) identify and understand risks associated with the asset – they do not have oversight or necessarily an understanding of the way technical systems are interacting;

2) mitigate risks to prevent incidents – they are not involved in physical operation and do not influence the risk management processes or disaster recovery plans;

3) minimise the impact of realised incidents – they are not physically capable of immediately responding to incidents; and

4) provide effective governance – they are not operationally close enough to implement risk management oversight, such as evaluation and testing.

It is therefore not appropriate that “financial” intermediaries be deemed to be Regulated Critical Infrastructure Entities. This function would be effectively performed by physical operators without obligations attaching to participants such as financial intermediaries. NEM registration may not always be the most appropriate point of imposing obligations.

2 Government Intervention

All participants in the identified sectors will be eligible for Government assistance. The Government will have the power to:

- **provide reasonable and proportionate directions** to entities when there is an imminent cyber threat or incident that could significantly impact Australia’s economy, security or sovereignty; and
- **take direct action** to protect a critical infrastructure entity or system in the national interest.

Telstra Energy agrees with the submission put forward by Telstra Corporation in Schedule 1 regarding appropriate safeguards being in place for these powers. It is important that Government intervention is applied with caution and only in very limited circumstances. The total investment required to achieve energy transition is beyond what could be feasibly funded by Government and heavy-handed intervention (short of complete centralisation and Government funding) runs the risk of making private investment less efficient.

In the Energy sector in particular, the sector-specific regulations must take into account the sophisticated regimes in the NEM around system security and supply. The National Electricity Law and Rules already have strict and very detailed regimes for ensuring power system security and minimising and mitigating the impacts of generators on that system. For example, AEMO has very broad powers of directions and the national energy regime has obligations around testing, maintenance and information provision. Any sector specific regulations should build on, but not duplicate or be inconsistent with, the existing energy protections in this area.

As discussed above, in the Energy sector, there are often many entities involved in an asset with varying roles and responsibilities. We consider that Government’s power to issue directions should also be limited to directions that entities are capable of complying with. This will ensure that directions are issued to the appropriate entity, which we consider would usually be the entity actually operating the asset.

As noted above, there should be a defence available to protect entities against improperly issued directions. Entities should not be liable for non-compliance with a direction to the extent that they are not legally or technically capable of reasonably complying with the direction. For example, financial intermediaries will generally not have the power to implement or change operational systems.