TELSTRA CORPORATION LIMITED

Register of critical telecommunications assets and mandatory cyber incident reporting—carrier licence condition

Public submission

29 March 2022

CONTENTS

01	**Overall telecommunications security regulation**	**3**
1.1.	Avoiding duplication and unnecessary regulatory burden	3
02	**Scope of the CLC requirements**	**3**
2.1.	Critical telecommunications assets	3
03	**Ownership and operational information**	**4**
3.1.	The ACMA register of carrier licences and nominated carrier declarations	4
3.2.	Clarifying what operational and ownership information is required by the Government	4
3.3.	Exemptions	4
04	**Mandatory cyber incident reporting**	**5**
4.1.	Existing processes	5
4.2.	Thresholds for cyber security incident reporting	5
05	**Additional comments**	**5**
5.1.	Grace periods	5
5.2.	Liability protections	5

01 Overall telecommunications security regulation

Telstra welcomes the opportunity to provide a submission in response to the Department of Infrastructure, Transport, Regional Development and Communications' (**DITRDC**) draft carrier licence condition (**CLC**). We support the Government's objective of the Critical Infrastructure and Systems of National Significance (**CI-SoNS**) reforms to uplift the security and resilience of the nation's critical infrastructure and have been an active participant in the consultation process for these reforms since mid-2020.

1.1. Avoiding duplication and unnecessary regulatory burden

A key focus for us has been to avoid any unnecessary duplication between the proposed reforms and the existing security obligations contained in Part 14 of the *Telecommunications Act 1997*, the Telecommunications Security Sector Reforms (**TSSR**). We support the Government's intention to achieve the critical infrastructure reform 'positive security obligations' through the Telecommunications Act for the telecommunications sector. This approach is intended to avoid duplication and introducing unnecessary regulatory burden.

To ensure the intention of avoiding duplication is achieved, we recommend the DITRDC consider the overall regulation of telecommunications security before implementing any security related changes to the Telecommunications Act. This could be achieved by expanding the 'phase two' consultation with the DITRDC and the Department of Home Affairs to capture the changes proposed in the draft CLC as well as the reforms relating to a risk management program and the Government's response to the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) report recommendations.[1]

For example, the ACMA's register of carrier licences and nominated carrier declarations already identifies ownership and operational arrangements for telecommunications networks in Australia. It is not clear to us what additional security benefit will be achieved by also providing this information to the Secretary of Home Affairs for inclusion in the Register of Critical Assets.

We also recommend that mandatory cyber incident reporting thresholds should be consistent with existing voluntary cyber incident reporting practices. Practically, this means aligning the threshold for reporting of 'other cyber security incidents' with the C2 level incident of the ACSC Incident Categorisation Matrix, which includes useful technical detail and thresholds for an important, but not 'serious' threshold cyber incident.

02 Scope of the CLC requirements

2.1. Critical telecommunications assets

We recommend that the requirements in the CLC be applied to critical telecommunications assets. The CLC requirements currently apply in relation to any assets of a carrier or CSP. An 'asset' is any tangible asset that is owned or operated by a carrier and used to supply a carriage service. Without limitation, this definition includes components of a telecommunications network, a facility, computer, computer device, computer program and computer data.

The Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (**SLACIP Bill**) narrows the *Security of Critical Infrastructure Act 2018* (**SoCI Act**) definition of 'critical telecommunications asset' to mean the networks and facilities owned or operated by a carrier/CSP and used to supply a carriage service. We propose that a consistent definition of critical telecommunications asset also be used in the

[1] Parliamentary Joint Committee on Intelligence and Security, *Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms*, February 2022.

CLC. This would introduce an appropriate criticality threshold while also reducing the burden to industry and Government of implementing the CLC security requirements. Importantly, the revised definition also better aligns with the objective of the CLC to improve the security and resilience of critical telecommunications infrastructure in Australia.

03 Ownership and operational information

3.1. The ACMA register of carrier licences and nominated carrier declarations

We recommend the Government rely on the ACMA's register of carrier licences and nominated carrier declarations to identify ownership and operational arrangements for telecommunications networks in Australia.

If the ACMA register is replaced by the CLC requirement, then we propose several practical changes to the CLC that recognise the complex nature of telecommunications assets:

- The requirement to provide operational and ownership information should apply only in relation to critical telecommunications assets (consistent with how that term is defined in the SLACIP Bill);
- Operational and ownership information can be consolidated (i.e. a single entry where the asset information is common across assets or classes of assets).
- Operational information can be updated annually for all assets instead of 30 days after each event (i.e. changes in exchange details are combined into a single annual notification).

These amendments aim to avoid the Secretary being provided with large amounts of irrelevant information about non-critical assets. This would serve no security benefit and place an unnecessary regulatory burden on both the carrier and Government.

3.2. Clarifying what operational and ownership information is required by the Government

Telstra welcomes additional clarity about the type of operational information carriers and CSPs need to provide under the CLC. The definition of 'operational information' lists several items and in most cases the requirement is clear. However, it is unclear to us what information would need to be provided in relation to '*the arrangements under which the carrier operates the asset*' or '*the arrangements for the maintained data*'.

In relation to the **maintained data** of an asset, it is not clear to us whether the intent here is to capture information about outsourcing and managed services arrangements? We would consider our data to still be maintained by us (including where we utilise third party contractors) whether we host our data on our premises, or in a private or public cloud environment. In all these cases we would retain control over that data.

3.3. Exemptions

We recommend that the CLC be amended to enable an entity or specified entities to receive an exemption from the requirement to provide operational and ownership information to the Home Affairs Secretary. This exemption from providing information for inclusion in the Register of Critical Assets applies to other critical infrastructure sectors under the SoCI Act.[2] A similar exemption from mandatory cyber incident reporting is also included in both the CLC and the SoCI Act.

[2] Section 27 of the SoCI Act enables rules to be made that exempt an entity, a specified class of entities or specified entities from complying with the requirements in Part 2

04 Mandatory cyber incident reporting

4.1. Existing processes

Telstra's cyber security team maintains a close operational and strategic working relationship with the ACSC. As a voluntary, business-as-usual activity Telstra provides updates and ongoing briefings on serious or potentially serious cyber security incidents impacting Telstra to the ACSC using existing processes. These updates and briefings are tailored for both operational and senior executive leadership teams and continue at a regular cadence as required or requested throughout any serious or potentially serious incident.

4.2. Thresholds for cyber security incident reporting

Telstra supports the reporting obligation definition and timeline for 'serious' cyber security incidents as outlined in the draft CLC. We recommend the threshold for reporting of 'other cyber security incidents' be set in line with the C2 level incident of the 2020 ACSC Incident Categorisation Matrix. With reportable incidents meeting a minimum standard of a C2 level incident.

This type of incident impacts national/critical national infrastructure and includes evidence of "Malware, beaconing or other network intrusion; temporary service/systems disruptions. Exfiltration or deletion/damage of key sensitive data or intellectual property, sustained disruption of essential systems and associated services." We believe this definition provides enough technical specifics to assist security teams determine thresholds for reportable incidents.

As it is currently drafted in the CLC, the threshold for reporting 'other cyber security incidents' could potentially capture a broad range of incidents and could lead to unnecessary volumes of reporting with no corresponding national security benefit.

Aligning with the C2 level incident of the 2020 ACSC Categorisation Matrix presents clear objective criteria and avoids unnecessary administration in relation to reporting on low level incidents.

05 Additional comments

5.1. Grace periods

We recommend that the mandatory cyber incident reporting obligation in the CLC includes a 3-month grace period. This timeframe is consistent with the grace period in the draft rules proposed under the SoCI Act to 'switch on' the mandatory cyber incident reporting obligation for other critical infrastructure sectors. Currently we are managing the reporting of serious and potentially serious cyber incidents to the ACSC using existing frameworks.

If the definition of 'other' cyber security incidents remains broad and without a meaningful threshold, we may need to develop new frameworks and technical capability to facilitate the transfer of an increased amount of data to meet this requirement. If this scenario were to eventuate, we would require at least a 3-month grace period to build and develop the required secure processes and capabilities to facilitate this requirement.

5.2. Liability protections

We recommend that the draft CLC includes the same statutory immunity provisions as the SoCI Act as amended by the SLACIP Bill) in relation to good faith compliance with mandatory cyber incident reporting obligations. This would ensure the same liability protections as other critical infrastructure sectors. It would also mirror the statutory immunity that is currently provided to carriers and CSPS in Part 14 of the Telecommunications Act in relation to good faith compliance with their TSSR obligations.

The SoCI Act[3] provides statutory immunity to entities (and officers, employees and agents) in relation to acts done in good faith in compliance with the mandatory cyber incident notification requirements in Part 2B. The SLACIP Bill extends this statutory immunity to acts done by related company groups and contracted service providers.

[3] Section 30BE (Liability) of the SoCI Act. The SLACIP Bill inserts new sections 30BE(3) and (4), extending this liability protection to acts done in good faith by related company groups and contracted service providers.