Department of Infrastructure, Transport, Regional Development, and Communications (the Department) Submission

Parliamentary Joint Committee on Intelligence and Security (PJCIS): *Review of the operation of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms*

Introduction

The Department of Infrastructure, Transport, Regional Development, and Communications (the Department) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS') inquiry into the operation of the Telecommunications Sector Security Reforms (TSSR), as set out in Part 14 of the *Telecommunications Act 1997* (Tel Act).

In making this submission, the Department notes the scope of the PJCIS' review, as specified by its report on the original bill[1], is on the operation, effectiveness and implications of the reforms introduced through TSSR. The PJCIS' report indicated that the review, would consider:

- the security of critical and sensitive data;
- the adequacy of information-sharing arrangements between government and industry; and
- the adequacy and effectiveness of the administrative guidelines in providing clarity to industry on how it can demonstrate compliance with the requirements set out in the Bill.

In preparing this submission, the Department has focussed on the *operation, effectiveness and implications* of TSSR, and provides views on whether further change is warranted. The Department's submission is structured as follows:

1. In part one, we outline the state of the telecommunications market, the role of the department, and why ongoing sustainable investment in the sector is critical to security.

2. In part two, we address the material improvement in the security posture of the telecommunications industry made under TSSR. Our view is that wholesale change of TSSR is not needed at this point, and could be counterproductive.

3. In part three, we present for the committee's consideration principles that could guide any future reform, and ideas that could further improve the operation of the framework.

The Department would welcome the opportunity for further engagement with the PJCIS, and would be pleased to provide more detailed information and analysis if the committee so desires.

[1] See also s315K of the Tel Act.

Part 1: The security and resilience of telecommunications is critical

The telecommunications market is critical to Australia's society and economy

Telecommunications are critical for Australia's modern society and economy. Whilst the telecommunications sector directly comprises only two per cent of Australia's Gross Domestic Product (GDP), it enables a further 25 per cent of GDP, and employs one per cent of the Australian workforce.

The importance of ready access to telecommunications was most acutely demonstrated during the bushfires that struck the nation earlier this year and during the COVID-19 crisis. During both of these periods, use of the telecommunications network to access government services, to be able to work from home and stay in touch with friends and family proved critical for the prosperity of the nation.

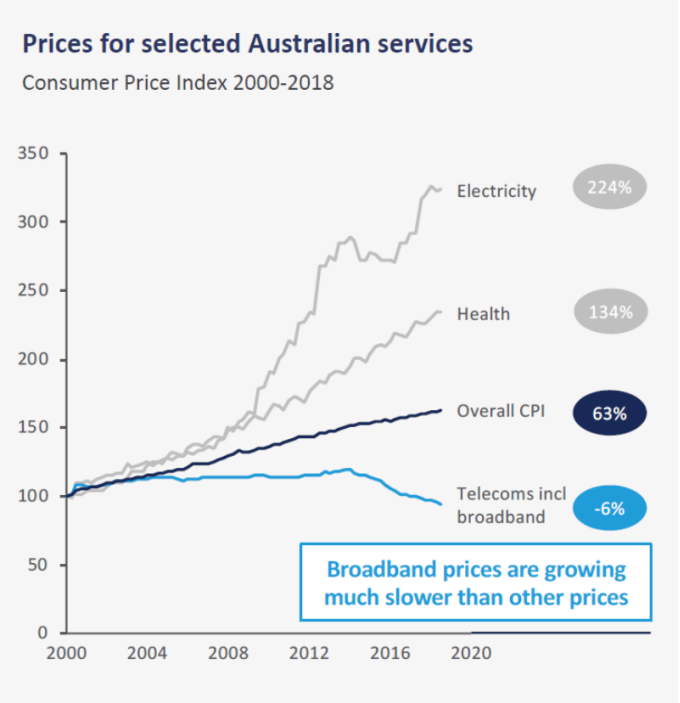
Our telecommunications networks were well placed to continue to serve the nation during these crises because of the substantial public and private sector investment that has occurred since the market was opened to competition in 1997. Since 1997, the number of carriers in the market has risen from a handful to over 300. The mobile network has seen substantial investment, with the three major carriers providing services to more than 99 per cent of the Australian population.[2]

The deployment of the National Broadband Network (NBN) has reached an important milestone – with the scale deployment of the network now complete, high speed fixed line broadband is now available at more than 11.7 million Australia homes and businesses. The Government's recent announcement, that NBN Co will invest a further $4.5 billion[3] in the network to bring fibre – and even better services – closer to homes and businesses is another important milestone. In addition, there is ongoing investment in backhaul networks by entities such as Vocus, Telstra, Optus and others. These network are not always front of mind but are critical to the ongoing functioning of Australian telecommunications networks.

Investment and competition across industries has delivered important outcomes for everyday Australians. The chart below shows the Consumer Price Index for the electricity, health and telecommunications sectors. As the chart demonstrates, compared to other sectors, competition has meant that despite substantial technological innovation and improved services, telecommunications prices have more or less remained stable over the past two decades.

[2] https://www.pc.gov.au/inquiries/completed/telecommunications/report
[3] https://www.nbnco.com.au/corporate-information/media-centre/media-statements/Initial-build-complete-NBNCo-announces-next-phase

The telecommunications industry is facing some complex challenges. These include declining average revenues per user (ARPU) across telcos'[4] customer base, the increased capital intensity of investment (particularly 5G investments) and the uncertain business case for new innovations including the ability to capture revenue from innovations. Net profitability is also trending down – industry will need to develop new innovations to build new profit centres. The Department has previously provided evidence of these factors in parliamentary submissions.[5]



It is also worth noting that the Australian telecommunications industry is diverse and that different firms face different challenges. This is true also from a security perspective – the security risks facing Mobile Virtual Network Operators, for example, are very different to the profile of backhaul providers or national mobile network operators.

Because of their critical nature, the security of telecommunications is paramount

Because of their critical nature, it is important that telecommunications networks are protected and are secure. Failure of the telecommunications network – because of sabotage, espionage or foreign interference (or even natural disasters) – can have a very real impact on Australia's economy and society. Threats facing the industry, and those that rely on the industry, relate to possible:

- compromise or degradation of telecommunications networks;
- compromise of valuable data or information of a sensitive nature, such as aggregate stores of personal data or commercial or other sensitive data (including telcos own data, and the data transmitted over networks by their customers);
- impairment of the availability or integrity of telecommunications networks; or
- impact on other critical infrastructure or government services (such as banking/finance, health or transport services).

As with any critical sector of the economy, the community expects high standards of security. Telecommunications networks, systems and facilities are also critical infrastructure and vital to the delivery and support of other critical infrastructure and services such as

[4] Referred to as 'telcos' for the purposes of this paper. Where this submission refers to 'telcos' it is generally referring to both 'carriers' and 'Carriage Service Providers' (CSPs). These terms are specified in section 7 and section 87 respectively, of the Tel Act.

[5] The PJCIS may be interested in the submission the Department provided to the Parliamentary inquiry into 5G telecommunications, available here: https://www.aph.gov.au/DocumentStore.ashx?id=b5678179-9962-44ee-8c18-43f303437dee&subId=673131

power, water and health (and vice versa). Consequently, failure of the telecommunications networks can have a domino effect across society and the economy.

The Department submits that it is primarily the telcos themselves that are best placed to protect their own networks from these threats. Telcos understand the configuration of their networks, they understand their supply chains, and they have very strong commercial incentives to maintain the resilience of their networks. A telco that cannot supply services to their customer base when they need it the most, is at risk of losing customers to their rivals. Consequently, telcos need to continuously invest in their network and introduce innovations and to guard against the threats that they know about. Likewise, it remains appropriate that regulatory interventions (such as TSSR) continue to place a primary obligation on industry to implement security controls.

The Department suggests that there are two primary roles for the Government:

1) Ensuring that the regulatory settings are such that telcos continue to have good incentives to invest in their networks, but in a secure way.

2) Ensuring that Government assistance is available so that telcos have good information about the threat landscape, and so that Government can intervene where it is in the national interest to do so. Telcos ability to protect against threats is dependent upon being aware of threats. The Government plays a key role in helping explain the threat landscape.

These twin objectives are being achieved in the Tel Act. The co-regulatory model provided by the Tel Act framework has meant that telcos continue to invest to improve their networks over the last two decades. The TSSR provides assurances to the community that the Government can intervene to ensure the security of Australia's telecommunications networks if needed.

The Department, and other entities in the framework, have a critical role to play

The Department is responsible for the design and implementation of the Australian Government's infrastructure, transport and regional development policies and programs, and is the lead agency for communications and the arts. The Department is the pre-eminent adviser to the Minister for Communications, Cyber Security and the Arts, and the Government more broadly, on the operation of the telecommunications market. Under the Administrative Arrangement Orders (AAOs), the Department is responsible for most telecommunications industry legislation, including the Tel Act itself.[6]

[6] The legislation administered by the Department is specified in the AAOs, (see https://www.legislation.gov.au/Details/C2020Q00003) and includes the Tel Act, the *Telecommunications (Consumer Protection and Services Standards) Act 1999*, the *Radiocommunications Act 1992,* Parts XIB and XIC of the *Competition and Consumer Act 2010* and others. The Tel Act comprises a number of parts relevant to security, including Parts 13 (protection of information), 14 (security of telecommunications), 15 (assistance and access) and 16 (disaster management).

The Department regards itself as a steward of the market, seeking to achieve the Government's policy objectives through market based mechanisms where possible. There are other Government and non-government bodies operating in the market that are important to achieve the policy objectives intended by TSSR. These include:

- The Australian Communications and Media Authority (ACMA): The ACMA is the telecommunications sectoral regulator, and is responsible for the registration of codes and standards created under Part 6 of the Tel Act. ACMA is also responsible for enforcement of much of the Tel Act, including the carrier licencing framework. ACMA's compliance and enforcement policy is available online.[7] Because ACMA is responsible for enforcement of the carrier licencing framework, it follows that its activities are critical to the success of TSSR.[8]

- The Department of Home Affairs (Home Affairs): Home Affairs is responsible for national security and law enforcement policy, and under the AAOs is responsible for administering, amongst other laws, the *Telecommunications (Interception and Access) Act 1979* and the *Security of Critical Infrastructure Act 2018*. Home Affairs is also responsible for the enforcement of TSSR, and has powers specified in Parts 30, 31 and 31A of the Tel Act to do so.

- Industry bodies: There are two principle industry bodies representing telcos and others associated with the telecommunications industry. These are the Communications Alliance (CA) and the Australian Mobile Telecommunications Association (AMTA). The operation of industry bodies is particularly important in the telecommunications market – the Tel Act is by design co-regulatory, and it is intended that industry (largely through industry associations) have a rule making function through the creation of codes, registered by ACMA under Part 6 of the Tel Act. Industry associations are also crucial in the policy development process for changes to the regulatory framework.

The Department is charged with ensuring that the framework and the activities of bodies in the market work together to support a vibrant telecommunications sector

[7] See https://www.acma.gov.au/compliance-and-enforcement-policy
[8] That is that unless the carrier licencing framework is enforced, and entities acquire carrier licences when required, TSSR cannot be effective.

Part 2: TSSR has been successful

TSSR continues to be effective.

The purpose of TSSR was to introduce a comprehensive risk-based regulatory framework to better manage national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities, and better protect networks and the confidential information stored on and carried across them from unauthorised interference and access. The aim was to encourage early engagement on proposed changes to networks and services that could give rise to a national security risk, and collaboration on the management of those risks.

The TSSR amendments formally commenced on 18 September 2018, following a 12 month implementation period. The TSSR framework is still relatively new, and so it can be difficult to determine how successful the framework has been to date. However, based on the information available to us – and we do consider that there may be some improvements to make (outlined in part 3 of this submission) – fundamental rework of the framework is unnecessary at this time.

There are two factors that we have considered when assessing the "*operation, effectiveness and implications*" of the framework:

1) Has the framework been effective in uplifting the security of telcos?

2) What has been the lived experiences of the entities operating in the system?

TSSR has resulted in a practical uplift in the security practices of telcos

As the Department notes above, it is the telcos themselves that are best placed to manage the security of their networks from threats that they are aware of. This does have an important caveat – telcos cannot protect their networks from unforeseen or unknown threats.

Thus, advice from Government – that has information about a broad range of threats – is critical. TSSR includes as part of its foundation, a requirement for telcos to notify the Critical Access Coordinator (CAC) of "a change that is proposed to a telecommunications service or a telecommunications system is likely to have a material adverse effect on the capacity of the carrier or provider to comply with its [positive security] obligations…".[9]

The CAC is located within Home Affairs, and has now had two years of experience in accepting notifications and facilitating the provision of advice to industry. The Department notes and fully supports the submission made by Home Affairs. We note that the Home Affairs' annual report records that for the first two years of TSSR's operation, that:

[9] See s314A.

- In the year to June 30 2020, CAC received 32 notifications under s314A(3), and in return issued 24 "some risk" notices and 6 "no risk" notices (2 were outstanding at 1 July 2020).
- In the year to June 30 2019. CAC received 34 notifications under s314A(3), and in return issued 28 "some risk" notices and 1 'no risk' (1) notices (5 outstanding at 1 July 2019).

That the CAC has been able to provide advice about risks in 52 of the 66 notices issued over the life of TSSR to date does suggest that there is valuable security information that is being transmitted to industry through the process. The Department notes Home Affairs' advice in its 2019-2020 annual report that:

"Most carriers [Home Affairs] has interacted with under TSSR are engaging positively with their obligations, including by:

- engaging in discussions to understand when the notification obligation applies;
- providing detailed information about changes to telecommunications systems and services via notifications; and
- participating in workshops to ensure best practice implementation of mitigations recommended in notices."

Moreover, telcos have also made commercial and operational decisions concerning the deployment of 5G networks as part of meeting their security obligation in TSSR. Some of these decisions demonstrate that TSSR has been effective in mitigating current and prospective security issues. It was also notable that such measures were undertaken by telcos following engagement through TSSR without needing enforcement or compliance provisions to be exercised.

Industry supports the continuation of TSSR

Since the introduction of TSSR, telcos have implemented technical and enterprise enhancements to support their engagement with security agencies, including Home Affairs as security regulator. These costs are now sunk, meaning that further change would require further funding, drawing telcos' investment away from other areas (such as improving coverage to rural Australia, or delivering price drops to consumers, or improving the redundancy and resiliency of their networks).

As noted above, the Department supports the submission made by Home Affairs, and further, notes that the submissions made by industry to proposed changes to the *Security of Critical Infrastructure Act 2018* (SOCI Act) could be of interest to the PJCIS in this context. We note that industry has indicated:

- Support for the underlying principles of security awareness, preparedness, and response;

- Support for other critical infrastructure and systems to adopt legislated security measures in a similar form to the security regulation of the telecommunications sector through TSSR;
- Acknowledgement of the general effectiveness of existing TSSR measures; and
- Caution about substantially changing the security environment for the telecommunications sector beyond enhancing the existing TSSR framework (for example, telecommunication companies suggested that it would be better to change TSSR in the Tel Act, if necessary, than to relocate telecommunication security regulation in entirety to the SOCI Act).

More information on central terms and the obligations of telecommunications entities in the Tel Act is provided in Appendix A. Information on the operation of TSSR is provided in Appendix B.

Part 3: Principles that could assist guiding future reform

The Department's view is that the security awareness shown by telecommunications entities and their willingness to fully support the principles embedded in TSSR indicate that TSSR is fundamentally fit-for-purpose. That does not mean that changes to TSSR, or security provisions more broadly, in the Tel Act should be ruled out. Changes in technology, geo-politics, communications services and forms, and in broader community expectations, should be reflected in the Tel Act itself over time, where appropriate, and where a balance can be struck with the other objectives of the Act, as set out previously.

The Department has developed a series of principles that we hope are useful for the PJCIS' deliberations. We consider that these principles may assist in determining whether change is needed to TSSR, and if so, what the parameters of that change ought be. We have developed these principles from the ground up, and so they start from the very basic to the more involved. They are:

1) **The ongoing investment and maintenance of telecommunications networks is essential to Australia's prosperity.** We consider that this is apparent from first principles – Australia is *prima facie* worse off without ongoing investment in telecommunications networks.

2) **The security of Australia's telecommunications networks is therefore paramount, as is a regulatory framework that promotes and permits ongoing sustainable investment.** If we consider that the ongoing requirement for telecommunications in Australia is paramount, then we submit that the security of telecommunications is also paramount.

3) **The telecommunications industry is best placed to manage their networks, including their security, if they have the information to do so.** Telcos can most effectively manage risk on and to their networks, if they have good information about risks and threats.

4) **The future is uncertain – technology changes, and geo-politics shift, but certainty is important for investor confidence**. Flexibility is needed to respond to changing environments, but predictability and proportionality of Government response is needed to promote investment and improve security. The Government can help by providing up-to-date threat information and continue to be transparent about future decisions and policy changes.

5) **Where regulation and powers may have significant impact on entities and potentially their customers/consumers in the telecommunications system, there must be appropriate civil protections, including the rule of law, natural justice, and judicial oversight.** One of Australia's competitive advantages compared to other destinations for investment is its strong institutional system. The rule of law, access to natural justice and independent judicial oversight make Australia an attractive

destination for ongoing domestic investment, and foreign investment where in the national interest, that ultimately improves the security and reliability of Australia's telecommunications.

6) **Any regulatory obligation and its costs should be proportionate to its benefit and the risk being faced and be implementable.** Ultimately dollars spent by industry in complying with regulatory obligations are dollars that cannot be spent on expanding and strengthening coverage, investing in research and development, implementing new security standards or lowering prices for consumers.

The Department hopes that these principles are of use to the PJCIS. The Department would welcome further engagement with the PJCIS on the practical ways that such principles could be implemented.

In this vein, the Department has developed three broad themes to capture areas of potential change. These themes, including some potential areas of exploration in each, are as follows:

1) Confirm and clarify the prominence of security as an obligation of carriers and carriage service providers.

The positioning and application of the security obligations of telcos within the Tel Act could be further improved, noting that substantial foundations already exist. Areas and options to explore could include:

<u>The objectives of the Tel Act</u>

- There is no object in s.3 of the Tel Act that specifically requires telecommunication carriers and providers to safeguard their systems and infrastructure from cyber and other security threats.
- At present the only object in s.3 which provides any support for security objectives is s.3(2)(h):

  (h) to provide appropriate community safeguards in relation to telecommunications activities and to regulate adequately participants in sections of the Australian telecommunications industry

- The addition of an object with a specific security focus would support the measures taken by Government and industry into the future. It would also mean that the full force of the existing regulatory framework (including codes and standards under Part 6 of the Tel Act, carrier licence conditions and service provider rules) could be available to support security objectives.

<u>The TSSR security obligation, and policy guidance to telcos</u>

- The current wording of the security obligation – that a telco must "do their best" – does not provide a clear standard to which each telco can be seen to meet.

- The creation of a delegated instrument (such as a determination making power), with appropriate Ministerial oversight, could offer a clearer alternative.
- Additionally, industry and government could create and promulgate security standards using existing mechanisms in Part 6 of the Tel Act which is currently used, for example, to set out emergency call service and mobile number porting identity requirements.

Security assessments undertaken at other points in the carrier licence process

- Absence of security checks at obvious trigger events (such as change of entity ownership or governance) may present a security gap.
- A change in ownership of a carrier, effectively a transfer of carrier licence, could trigger a security check subject to a risk assessment.

2) Security obligations should be supported by sound and effective enforcement and compliance mechanisms

This theme recognises that telcos' obligations to meet security standards and requirements should be supported by appropriate powers. Some ideas for improvements against this objective could include:

Applying the 'direction power' based on the best advice of where the security risk lies

- As currently written, the directions power must only be used in respect of an Adverse Security Assessment furnished on that telco. Where the security risk lies with another entity, it could be appropriate that the Government is able to direct the telco in relation to that entity (for example, a supplier of IT systems).

Using the TSSR enforcement and compliance framework to enforce security-related carrier licence conditions and service provider rules that have a security objective

- There are a range of mechanisms in the Tel Act that could be used to resolve security issues. These include the creation of carrier licence conditions, service provider rules and codes/standards under Part 6 of the Tel Act.
- If these mechanisms are used to achieve security objectives, it is appropriate that the Minister for Home Affairs have the ability to enforce these obligations, consistent with the powers that the Minister for Home Affairs already has in relation to TSSR.

Increasing the visibility of CSPs that deliver specific services most at security risk

- Existing legislative mechanisms in the Tel Act (such as licence conditions or service provider rules) could be used to increase visibility of CSPs that deliver specific services most at security risk.
- Whilst carriers are visible through the licence regime, there is no list of CSPs of interest, should a regulator need one for proactive enforcement.

- A list of a subset of CSPs delivering specific services, such as commercial telephony or broadband services, could be maintained by either regulator (CAC or ACMA) and be used to proactively enforce security, consumer protection and other obligations across the Tel Act.

3) Improve situational awareness and ensure the regulatory burden on telcos is transparent and proportionate

This theme seeks to ensure that the framework encourages information sharing and oversight of security risks, gaps and threats, while providing effective governance over the regulatory framework as a whole.

Improve situational awareness across Government and industry on security threats and issues.

- Existing mechanisms such as the Trusted Information Sharing Network (TISN) could be reinvigorated and established to better facilitate the sharing of sensitive security risks.

- Streamline the notification process in TSSR to make sure the Government receives timely and appropriate advice on security threats known to industry, while reducing the regulatory burden.

The regulators of the Tel Act for security obligations and associated provisions (the CAC and ACMA) could establish enforcement and compliance frameworks.

- Compliance frameworks (or plans) could be used to set out the enforcement and compliance strategies and actions as identified by the regulators.

Conclusion

The Department trusts that this submission has been of some use to the PJCIS' deliberations.

In summary, the Department puts to the committee that:

1) Ongoing investment in telecommunications networks is critical for Australia's continued prosperity.

2) The security of these networks is therefore critical. Regulatory setting that permit ongoing sustainable investment are likewise critical, as are settings that maintain a high degree of security in networks.

3) It is appropriate that the private sector remain primarily responsible for managing the security of their networks.

4) It is likewise appropriate for the Government to encourage investment in the industry to improve security and for the Government to impose standards for industry to comply with.

5) The future is uncertain, and it is appropriate that the current framework is maintained, with it substantial flexibility.

The Department would welcome further engagement with the PJCIS on these and other matters. We would be grateful for the opportunity to discuss the issues raised in this submission. The contact officer in the Department for this matter is [redacted], Assistant Secretary, Telecommunications Market Policy Branch. [redacted]

Appendix A: Outline of key provisions of the Tel Act

Central terms

There are a range of central terms spelt out in the Tel Act. These terms begin at a very granular level and are built up through accumulated definitions. These central terms are explained below in the context of the key entities outlined above – carriers, CSPs and Content Service Providers. Real world examples are shown where appropriate. Defined terms in the Tel Act are in ***bold italics*** in the first instance.

*a) What is a **carrier**?*

A carrier is an entity that owns physical telecommunications infrastructure used to supply a ***carriage service*** to ***the public***. To be captured, this infrastructure must be a ***network unit***.

- A network unit is a:
  - ***Line/Line link***: A line is a wire, cable or similar infrastructure for carrying communications by guided electromagnetic energy (EME) connecting at least two ***distinct places*** in Australia by at least the ***statutory distance*** (500 meters). A line link is a device that connects two lines (i.e. two lines connected by a line link are a single network unit). A line is not a network unit to the extent it is on the customer side of the network boundary[10].

The identification of 'distinct places' can be complex. Two places on the same freehold or leasehold parcels of land are not distinct places. Two points on a beach, or two points in the sea are not distinct places because they are on unalienated Crown land.

  - ***Designated radiocommunications facility***: This includes a mobile base station, satellite facility or other similar facility.

Examples of equipment that can be regarded as a network unit include[11]:

- A **mobile base station** that is part of a public mobile network (i.e. a Telstra base station to supply voice or data or a TPG base station only supplying data).[12]
- A **wireless router** supplying services to the public on a commercial basis.[13]

[10] The ***Boundary of a telecommunications network*** is determined through regulation, or if no regulations are made (none are) through agreement between the customer and the carrier or CSP, or failing agreement, the main distribution frame (MDF), the outer surface of satellite facility, or failing those options the outer surface of a fixed facility. This would include: wall plate of a fixed line facility, the MDF in an apartment block, the satellite dish for a satellite service, the wireless modem/dongle used for mobile broadband or services.
[11] The examples would be caught so long as other criteria are met – i.e. supply to the public.
[12] See s31(1)(a).
[13] See s31(1)(c). Note that services provided on a non-commercial basis would be caught but for a long standing ministerial exemption that has been put in place.

- A **cable** that stretches more than 500 m from one property to another supplying a service outside of the cable owner's immediate circle.[14]
- A **satellite dish**, either transmitting or receiving as long as it is supplying carriage services outside of the immediate circle.[15]

- A carriage service is "a service for carrying ***communications*** by means of guided and/or unguided electromagnetic energy". The term communications has a broad meaning, and include communications that are otherwise undecipherable by humans (such as binary code or encrypted data) as long as the information can be interpreted by a human or a machine. The term electromagnetic energy has its natural meaning and includes light, electricity and radiation.

  Services that can be regard as carriage services:

  - An encrypted **email**.
  - An **instant message**.
  - A **telephone call**.
  - A **video stream**.
  - **Wireless commands** from one machine to another (i.e. a Google Nest network).

- The supply of a carriage service to the public. The meaning of 'to the public' has different meanings depending on the situation – generally supply of a carriage service outside of the carrier's ***immediate circle*** would be captured. The immediate circle are all entities that fall within a corporate structure.[16] This can include an individual and their employees, a corporation and their parents and subsidiaries, a Government and their agencies. This definition means that if a corporation supplies services to itself or subsidiaries (i.e. a corporation supplies an internal message service to its employees), this service is not captured.

  Examples of entities **inside** the immediate circle of a corporate body:

  - A **business unit** in the same business (i.e. the accounts department of a carrier)
  - A **subsidiary**
  - A **parent company**
  - **Contractors and employees**

The Tel Act framework provides for exemptions for certain categories of telecommunications networks.[17] This includes:

- Networks operated by Defence;
- Networks operated by the Australian Secret Intelligence Service (ASIS), Australian Security Intelligence Organisation (ASIO) and Australian Signals Directorate (ASD);
- Transport authorities (aviation, rail and state and Territory transport authorities);

[14] See ss26 and 30.
[15] See ss7, 28 and 30(d)
[16] See s 50 of the *Corporations Act 2001*
[17] See ss 45 – 50.

- Entities providing broadcasting services;
- Electricity supply services; and
- Historical legacy networks that were carved out of the 1975, 1989 and 1991 Telecommunications Acts.

*b) What is a **CSP**?*

A CSP is an entity (including a natural person) that supplies (or proposes to supply) a ***listed carriage service***[18] to the public.[19] A person that supplies or proposes to supply a listed carriage service using a line link from one point in Australia to a place outside of Australia or that uses a satellite-based facility is also CSP. A person that supplies a listed carriage service to the public using a network unit exempt from requiring a carrier licence is also a CSP.[20]

A person who for reward arranges, or proposes to arrange for the supply of a listed carriage service, to a third party is a ***Carriage Service Intermediary***, which is also a CSP.

There are a range of exemptions in the Tel Act. These include services provided by[21]:

- Customers located on the same premises;
- Defence;
- The Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO) and the Australian Signals Directorate (ASD);
- Transport authorities;
- Broadcasters; and
- Electricity supply bodies.

As a general statement, CSPs attract a number of regulatory obligations across the Tel Act. See, in particular, Parts 6, 13, 14, 15, 16, 17 and 18. The ACMA also has powers to create service provider rules, which could then be used to impose additional obligations.[22]

*c) What is a **Content Service Provider**?*

A content service provider[23] is a person that uses or proposes to use a listed carriage service to provide a ***content service***. A content service is:

- A broadcasting service;
- An on-line information services (the example given in the Tel Act is a dial-up information service – a website would be a modern equivalent);

[18] A listed carriage service is a carriage service provided between two points in Australia and a carriage service between multiple points in Australia and outside Australia as long as there at two points in Australia, and a carriage service to multiple points in Australia and outside Australia as long as there one point is in Australia and at least one point is outside of Australia. The meaning of 'point' includes mobile points (i.e. a vehicle or aircraft), including in outer space, underground or underwater.
[19] That is - outside of the entities immediate circle.
[20] See s87(3).
[21] See ss89 – 94.
[22] See s99.
[23] See s97.

- An on-line entertainment services (i.e. an online game or a streaming video service);
- Any other on-line service.

For the purposes of the Tel Act, a content service is supplied to the public, if and only if, one user of the content service is outside of the immediate circle of the supplier of the content service.

The content service provider definition is a latent definition in the Tel Act, in that content service providers do not attract any regulatory obligations at present. However, the ACMA has powers to create service provider rules, which could then be used to impose regulatory obligations.[24]

[24] See s99.

Appendix B: The operation of TSSR in Part 14 of the Tel Act

Overview of the existing security obligations of telecommunications entities in the Tel Act

On 15 September 2017 the Parliament of the Commonwealth of Australia passed the *Telecommunications and other Legislation Amendment Bill 2017* (the Bill). The Bill received Royal Assent on 18 September 2017. The resulting legislation, titled the *Telecommunications and other Legislation Amendment Act 2017*, amended the Tel Act and related legislation. The amendments formally commenced on 18 September 2018, following a 12-month implementation period. These amendments are generally referred to as the Telecommunications Sector Security Reforms (TSSR).

The Act stipulates that a change to a telecommunications service or a telecommunications system includes (but is not limited to) Carriers and nominated CSPs (C/nCSPs) [25] making the following changes:

- providing new telecommunications services;
- changing the location of telecommunications equipment and network management equipment (including moving equipment outside Australia);
- procuring telecommunications equipment and network management equipment (including procuring equipment that is located outside Australia) where the equipment forms or supports 'sensitive parts of networks'[26];
- entering into outsourcing arrangements,
    - to have all or part of the telecommunication services provided for a C/nCSP, or
    - to have all or part of the provision of telecommunication services managed for a C/nCSP, such as managed services for the management of all or some of C/nCSP's telecommunications data;
    - or the management of all or some of C/nCSP's telecommunications data.
- entering into arrangements to have all or some of its telecommunications information accessed by persons outside Australia; and

[25] A nCSP is nominated under s.197(4) of the *Telecommunications (Interception and Access) Act 1979*

[26] Notifiable equipment includes equipment that is essential to the C/nCSP's telecommunications system or the provision of its services. Any equipment that manages confidential information is notifiable.

- entering into arrangements to have all or some information or documents to which subsection 187A(1) of the *Telecommunications (Interception and Access) Act 1979* applies kept outside Australia.

In addition to the above types of changes being listed in the Act, public guidance material[27] provided by the government recommends that C/nCSP's also notify of the following types of changes:

- changing the levels of access to, or control of, sensitive data or information, including customer data;
- changes in access to facilities or systems, such as providing third party access to facilities;
- replacing mission-critical operational software, even if on a like-for-like basis;
- introducing a new supplier into the supply chain, even if the new supplier is supplying the same or similar goods or services as previous supplier/s;
- where new equipment is being supplied that affects a significant number of people or customers; and
- changing the management of services, including new contractual arrangements and third parties, or when key outsourcing arrangements are first renewed since TSSR came into effect.

Furthermore, the guidance recommends that C/nCSPs do not need to submit notifications for changes that do not affect their capacity to comply with their security obligation. Examples include:

- replacing equipment with similar or upgraded versions, where it is sourced from the same vendor; and
- day-to-day changes, such as routing changes or software updates.

TSSR also gives the Minister for Home Affairs two directions powers, namely:

1. to give the carrier or carriage service provider a written direction not to use or supply, or cease using or supplying, the carriage service(s) if the Minister considers that the proposed use or supply would be, or the use or supply is, prejudicial to security;[28]
2. to give a carrier, carriage service provider or a carriage service intermediary a written direction to do, or refrain from doing, a specified act that is reasonably necessary to eliminate or reduce the risk of unauthorised interference with, or unauthorised access to, telecommunications networks or facilities that would be prejudicial to security.[29]

[27] Telecommunications Sector Security Reforms Guidance
[28] See s.315a
[29] See s.315b

The exercise of these directions powers is subject to various safeguards. For example, a prerequisite is the existence of an adverse security assessment by the Australian Security Intelligence Organisation.[30]

TSSR also empowers the Secretary of the Department of Home Affairs to obtain information or documents from carriers, carriage service providers and carriage service intermediaries to assess their compliance with the security obligation.[31]

The relevant TSSR guidelines indicate that following the submission of a notification the carrier or nominated carriage service provider will receive one of the following notices from the CAC:

- A **request for further information** about the proposed change so the CAC can assess whether there is a risk of unauthorised access to, or interference with, telecommunications networks or facilities that would be prejudicial to security.
- A **notice advising of a risk** associated with the proposed change of unauthorised access to, or interference with, telecommunications networks or facilities that would be prejudicial to security. In this situation the CAC will seek to engage the carrier or nominated carriage service provider to discuss and determine appropriate measures to reduce or eliminate the risk of interference or unauthorised access.
- A **notice advising that the CAC is satisfied there is not a risk** from the proposed change of unauthorised access to, or interference with, telecommunications networks or facilities that would be prejudicial to security.[32]

The CAC assesses notifications on a case-by-case basis, taking into account all the relevant facts and circumstances.

[30] See Tel Act s.315a(3) and s.315b(4); s.37 and s.38A of the *Australian Security Intelligence Organisation Act 1979*
[31] See s.315c
[32] Notification requirement fact sheet Version 1.0 published 11 October 2018