Australian Government
Department of Home Affairs

Department of Home Affairs submission to the statutory review of Part 14 of the *Telecommunications Act 1997*

Parliamentary Joint Committee on Intelligence and Security

November 2020

Table of Contents

Introduction

1. The Home Affairs Portfolio welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) statutory review of the operation of Part 14 of the *Telecommunications Act 1997* (Act), to the extent that Part 14 of the Act was amended by the *Telecommunications and Other Legislation Amendment Act 2017*, known as the Telecommunications Sector Security Reforms (TSSR).
2. Home Affairs Portfolio provided this unclassified submission with input from the Australian Security Intelligence Organisation (ASIO).
3. This submission provides an overview of the operation of TSSR in respect to the four key elements of the framework with a focus on the operation, effectiveness and implications of the reforms. The submission addresses the following areas of focus as set out by the PJCIS:
    - 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 TSSR.

Context

4. The security and resilience of telecommunications infrastructure significantly affects Australia's national security, economic prosperity and social well-being. Government and businesses are increasingly storing and communicating large amounts of information on and across telecommunications networks and facilities. By their nature, telecommunications networks and facilities hold and transmit sensitive information. Telecommunications networks, systems and facilities are not only critical infrastructure in themselves, but are vital to the delivery and support of all other critical infrastructure sectors and services.
5. For these reasons, telecommunications networks and facilities, and the carriers and carriage service providers (C/CSPs) that own or operate them, are attractive targets for espionage, sabotage and foreign interference activity by state and non-state actors.
6. National security risks associated with telecommunications networks and facilities relate to possible:
    - unauthorised access to telecommunications networks or facilities;
    - unauthorised access to communications or to valuable, sensitive data;
    - unauthorised interference with the integrity or availability of telecommunications networks or facilities, or the data they hold or carry; or
    - consequences for dependent critical infrastructure and services, such as banking and finance, health or transport services.
7. In addition to national security risks, Australia has seen an increase in complex natural disasters that have cascading effects on critical infrastructure assets, including telecommunications infrastructure. These hazards have the potential to significantly compromise the supply of essential services across Australia. Home Affairs is working with the telecommunications sector to ensure our practices, policies and legislation bolster the security and resilience of our telecommunications networks and systems which will allow us to act in future emergencies.
8. Prior to the commencement of TSSR on 18 September 2018, managing national security risks in the telecommunications sector was largely achieved through informal cooperative arrangements with industry. There were significant limitations to this approach as it was only workable where companies were willing to give due consideration to national security and the public interest. This meant that security costs were borne only by market participants who chose to do so. By contrast TSSR applies equally to all C/CSPs in the telecommunications market and as such, creates a level playing field across the market.

9. The Telecommunications and Other Legislation Amendment Bill 2016 (the Bill) amended the Act and related legislation, to introduce the TSSR framework to better manage these national security risks to Australia's telecommunications networks and facilities.

10. TSSR has been implemented by the Critical Infrastructure Centre (the Centre) within the Department of Home Affairs (Home Affairs), supported by advice from national security agencies such as ASIO and the Australian Signals Directorate, and in collaboration with the Department of Infrastructure, Transport, Regional Development and Communications.

11. TSSR is a principles based framework that formalises the good faith engagement between Home Affairs and Australia's telecommunications sector to better manage national security risks to telecommunications networks. The TSSR framework is intended to encourage early engagement on proposed changes to networks and services that could give rise to national security risks and collaboration on the management of those risks.

12. Home Affairs appreciates the engagement and collaboration it has with the telecommunications sector. We take this opportunity to acknowledge that the management of national security risks would not be possible without a solid foundation of trust and good faith engagement between the telecommunications sector and Government.

Supply Chain Security

13. A key source of vulnerability of telecommunications networks and facilities is in the supply of equipment, services and support arrangements. Australian telecommunications providers rely on the global supply of equipment and managed services which can create further challenges in implementing controls to mitigate personnel, physical and information security risks. These risks can lead to telecommunications networks and facilities being more vulnerable to unauthorised access and interference.

14. Supply chains can be interrupted or distorted by a range of issues, from malicious cyber activity and supplier insolvency through to coercion and international trade disruptions. Although many businesses are aware of these risks, and may already have strategies in place to combat them, the geostrategic environment is changing rapidly.

15. The COVID-19 pandemic has highlighted the potential vulnerabilities of supply chains for telecommunications equipment and services. Home Affairs acknowledges the disruption the pandemic has caused to the supply chain and the working arrangements for the telecommunications sector who manage network operations and security, in particular, the movement of specialist technicians and equipment across state and territory borders. Home Affairs would like to take this opportunity to acknowledge the ongoing engagement from the telecommunications sector during this period.

16. Advances in technology and telecommunications have introduced new vulnerabilities, including new methods to compromise the confidentiality, integrity and availability of telecommunications networks and associated critical infrastructure and the sensitive information held on these networks. These vulnerabilities can allow state and non-state actors to obtain unauthorised access to networks.

17. The Home Affairs Portfolio is also aware of the potential sustainment risks associated with the United States' export restrictions affecting certain telecommunications equipment and component vendors. Home Affairs continues to engage with mobile network operators to understand and manage these and other risks. Home Affairs routinely engages with owners and operators of telecommunications infrastructure, including States and Territories, on privacy, security and law enforcement issues, including supply chain security. Home Affairs works collaboratively with the sector to identify these risks on a case-by-case basis via the TSSR regime.

5G

18. Telecommunications networks will increasingly underpin other critical infrastructure sectors with wide applications across industries. The unique capabilities of 5G can open up new opportunities to support critical infrastructure systems within smart cities, the increased use of the Internet of Things (IoT), industrial control and safety of life systems, such as real-time monitoring of patients, in-body internet

connected devices and autonomous vehicles. These rapidly evolving technologies make telecommunications networks an even more attractive target for espionage, sabotage and foreign interference activity by state and non-state actors.

19. Government is focused on creating the enabling policy and regulatory environment to facilitate and accelerate the deployment and take-up of 5G, so Australians can realise the full benefit of 5G technologies, while ensuring that Australia's information and communications are protected from espionage, sabotage and foreign interference activity at all times.

20. Following an extensive review, guidance on 5G security was provided to the Australian telecommunications sector on 23 August 2018. Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference. Government has set its expectations of the application of the TSSR obligations with respect to the involvement of third party vendors in 5G networks, including the evolution of networks that lead to mature 5G networks. Australia's 5G security posture is fundamentally underpinned by the TSSR regime.

Protecting Critical Infrastructure and Systems of National Significance Reforms Package

21. The Australian Government is committed to working with industry to maintain the security and resilience of assets, networks and systems that are critical to Australia's social and economic stability, defence and national security.

22. On 6 August 2020, the Minister for Home Affairs announced the Protecting Critical Infrastructure and Systems of National Significance (CI/SONS) Reforms Package as part of the release of the *Cyber Security Strategy 2020.* On 12 August 2020, the Minister released a consultation paper to seek the views of industry on key elements of the reform package.

23. The reform package seeks to broaden the existing scope of the *Security of Critical Infrastructure Act 2018* (SOCI Act) to capture additional assets in eleven sectors of the economy, and to introduce the following mechanisms:

- **positive security obligations (PSO)** which includes three elements:
  - the expansion of the *register of critical infrastructure assets* to provide Government with greater visibility of the ownership structure and operational arrangements of a broader range of critical infrastructure assets;
  - mandating *risk management programs* that identify hazards that could impact the availability, integrity, reliability or confidentiality of critical infrastructure assets, minimise or eliminate such hazards from occurring, and mitigate the impact of such hazards on the critical infrastructure asset; and
  - a requirement to report *cyber security incidents* to provide Government with an aggregated threat picture and comprehensive understanding of cyber security risks.
- **government assistance measures** to permit the Government to provide active assistance as a last a resort in response to the most serious of cyber security incidents that are impacting a critical infrastructure asset and Australia's national interest.
- **enhanced cyber security obligations** for the highest criticality assets, to enable Government to request information to contribute to a near real-time national threat picture, owner and operator participation in preparatory activities with Government, and the co-development of a scenario based 'playbooks'.

24. It is intended for assets currently regulated under the TSSR framework to be captured as critical infrastructure assets under the reform package. This will ensure that, if passed by Parliament, the government assistance measures can be used to address a cyber security incident impacting those assets that are essential to the provision of communications services.

25. As currently envisaged, the positive security obligations must be activated for individual assets, including through the creation of rules by the Minister for Home Affairs. The Government will consider the outcomes of this statutory review and conduct further industry consultation when implementing the proposed amendments to the SOCI Act (see paragraphs 32-34 and 62 below).

TSSR Framework

Security Obligation

26. Subsection 313(1A) and 313(2A) of the Act requires C/CSPs and carriage service intermediaries (CSIs) to, for the purposes of security, 'do their best to protect the networks they own, operate or use, from unauthorised access or interference to ensure the availability and integrity of telecommunications networks and facilities; and the confidentiality of communications carried on, and information contained on telecommunications networks or facilities' ('the security obligation').

27. Subsection 313(1B) of the Act requires C/CSPs (but not CSIs) to maintain competent supervision and effective control over telecommunication networks and facilities that they own or operate.

28. The security obligation applies only to a subset of the Australian telecommunications sector and does not apply to overseas over-the-top (OTT) services or entities in the supply chain. Telecommunications networks operated by transport or energy entities are typically exempted from obligations under the Act, unless the operators of those critical infrastructure assets choose to acquire a carrier licence for their own reasons. Subject to passage of amendments to the SOCI Act, certain assets in the energy and transport sectors are intended to be captured as critical infrastructure assets. As such, these assets (including their private telecommunications networks) may be subject to the PSO obligations if these are relevantly activated.

29. For the purposes of the security obligation, 'security' has the same meaning as in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act).

30. The security obligation is focused on managing telecommunications networks and facilities from unauthorised access and interference, but does not specifically outline security requirements such as:

- detecting malicious activity;
- taking proportionate and necessary action to protect all systems;
- mandatory incident reporting;
- maintaining resilience and risk mitigations to minimise the impact of malicious activity; and
- participating in cross-sectoral exercises.

Challenges with the security obligation

31. The subjective nature of the term 'do your best' has proven challenging to implement. This is because it fails to outline any specific measures or practical protections that C/CSPs and CSIs must implement in order to meet their security obligation. This creates uncertainty within the telecommunications sector as to how it is to meet its obligations.

Potential enhancements

32. A more specific, positive security obligation that is underpinned by specific guidance would give certainty and consistency to both Government and industry. Noting that telecommunications remains a key sector of critical infrastructure, a positive security obligation consistent with the sector specific standards proposed for sectors captured by the draft Security Legislation Amendment (Critical Infrastructure) Bill 2020 and proportionate to risk could set and enforce appropriate baseline protections against all hazards for telecommunications systems and facilities.

33. Such a positive security obligation would also ensure that C/CSPs implement and maintain appropriate governance and risk management oversight that includes a robust assurance and review process. In addition to the positive security obligation and complementary to the CI/SONS reforms for other sectors,

mandatory cyber intrusion reporting requirements for carriers as proposed in the draft Security Legislation Amendment (Critical Infrastructure) Bill 2020 would provide Government with the ability to develop a near real-time threat picture and comprehensive understanding of cyber security risks. In the telecommunications sector these cyber security risks have the ability to create cascading consequences for all critical infrastructure sectors.

34. These proposed obligations should not displace the current notification obligation in s314A of the Act. The TSSR notification regime was introduced in recognition of the heightened risks and extreme consequences of disruption to our telecommunication networks. Government will continue to need visibility of upcoming changes to networks in order to provide appropriate risk advice on a case by case basis.

Notification Obligation

35. The notification obligation in section 314A of the Act requires all carriers and nominated carriage service providers (C/NCSPs) to notify the Communications Access Coordinator (CAC) of proposed changes to their telecommunications systems or services if they become aware that the proposed change is likely to have a 'material adverse effect' on their capacity to comply with the security obligation.

36. The notification obligation is intended to formalise information sharing between C/NCSPs and Government and reflects Government's interest in working with C/NCSPs to protect the security of our telecommunications networks. The notification obligation provides a mechanism for Government to understand how a C/NCSP is meeting their security obligation in relation to proposed changes in the context of the national security threat landscape and with regard to privileged information held by Government. The notification obligation also advises the CAC of a C/NCSP's mitigations to manage identified risks.

37. A notification form is available on the Critical Infrastructure Centre website to provide guidance on the type of information to be included in the notification. Through the notification process, the CAC specifically seeks the following information about data assets as they relate to the proposed change:

- Data assets such as Personally Identifiable Information (PII), billing records and system configuration details;
- Physical location of the data, including country details if the data is hosted offshore and/or by a third party;
- Access to the data, including any third parties;
- Any risks to the confidentiality and integrity of the data, as identified by the C/NCSP; and
- The security controls the C/NCSP has in place or proposed to put in place to mitigate the identified risks.

38. Home Affairs works closely with security agencies to assess notifications and to share current threat and vulnerability information as relevant to the proposed change that the C/NCSP would not normally have access to. The notification process allows Home Affairs to provide information that is often specific and technical in nature such as risks related to equipment supply, outsourcing and offshoring arrangements and controls to manage identified risks. Submitting a notification allows C/NCSPs to benefit from the information Government has available to it and ensures C/NCSPs can make informed decisions about any proposed changes.

39. As at 30 June 2020, Home Affairs has received 66 notifications under subsection 314A(3) of the Act since TSSR commenced on 18 September 2018. The notifications received from carriers to date represent the vast majority of the fixed-line and mobile telecommunications market in Australia.

Limitations of the notification regime

40. Home Affairs notes that there has been some variation among C/NCSPs in their approach to the TSSR notification obligation. The obligation relies on self-determination by C/NCSPs of whether a proposed change warrants a notification, regardless of the guidance provided by Home Affairs. There have been

instances where Home Affairs has engaged with a carrier about a proposed change to their networks and subsequently recommended that the carrier submit a notification as it was Home Affairs' view that the features and characteristics of the proposed change introduced significant risk. Despite Home Affairs' recommendations to these carriers, they did not proceed to submit a formal notification; in the carrier's view, the proposed changes to their networks or facilities did not meet the carrier's internal risk assessment thresholds for formal notification. In the absence of a notification, Government has no visibility of changes to networks or steps taken to mitigate risks and cannot provide advice.

41. In the above situation, not notifying Home Affairs about a proposed change does not prevent Government taking action. While Home Affairs' primary focus is to achieve national security outcomes on a cooperative basis, the Act allows the Minister for Home Affairs to seek an injunction requiring a notification, accept an enforceable undertaking or pursue civil penalties in relation to non-compliance with s314A(3) of the Act. However, there is significant administrative and financial burden associated with these enforcement measures and may not be the most appropriate mechanism to achieve an appropriate security outcome.

42. It is Home Affairs' view that submitting a notification is one way in which C/NCSPs can demonstrate that they are complying with their security obligation by looking to make an appropriately informed decision about whether to implement a proposed change. Submission of a notification indicates that the C/NCSP is aware that the proposed change may adversely affect its ability to comply with its security obligation and is not an admission that the C/NCSP is proposing to breach its security obligation or to do an act that is prejudicial to security. However, the current phrasing of s314A has led to concerns within some carriers that a notification is an admission of a breach of security. In particular, the words 'likely to have a material adverse effect on the capacity of the carrier or provider to comply with its obligations under subsection 313(1A) or (2A)' have led some carriers to conclude that s314A requires them to have decided to breach their security obligation before triggering the notification threshold, and note that this is not a decision they would make in any circumstances. While this is not Home Affairs' understanding of the wording in s314A, clarifying the notification threshold would assist to dispel this concern and ensure changes are being appropriately notified as intended under the TSSR regime.

43. There are also challenges associated with the response options available to Home Affairs. The CAC has 30 calendar days to assess if a proposed change presents a relevant risk, being the risk of unauthorised access to or interference with, telecommunications networks or facilities that would be prejudicial to security. The CAC may respond to the C/NCSP with either:

    - a request under subsection 314B(1) of the Act for further information in relation to the proposed change;
    - a notice under subsection 314B(3) advising that the CAC has identified a relevant risk in relation to the proposed change; or
    - a notice under subsection 314B(5) advising that the CAC is satisfied that there is no relevant risk associated with the proposed change.

44. If the CAC considers that where a notified proposed change carries a relevant risk, the current legislation is silent on allowing Government to do anything more than advise the carrier what those risks are and suggest mitigations to address them. The CAC is unable to enforce mitigations upon the carrier without resorting to Ministerial directions powers or civil proceedings. Additionally, there is no formal mechanism to acknowledge satisfaction that the risks identified by the CAC in relation to the proposed change have been adequately addressed. The C/NCSP is also not required to inform the CAC how (or if) it has implemented any suggested mitigations. While voluntary engagement can resolve some of these concerns, this depends on the willingness of the C/NCSP and in Home Affairs' view may not give appropriate certainty to Government and the public that the identified risks are being addressed.

Potential enhancements

45. Home Affairs suggests additional types of notices with more nuanced language to reflect various levels and types of risk, and the urgency of adopting further mitigations. For example, the framework does not currently allow issuing of a notice where the CAC acknowledges there is risk with a proposed change and the C/NCSP intends to implement mitigations which the CAC has found to be proportional to the risk.

46. Amending the Act to allow Home Affairs to request a notification about a proposed change, including in circumstances where a C/NCSP has internally determined that it need not notify, would ensure that any changes to telecommunications networks and systems does not introduce national security risks.

47. Amending the Act to give Home Affairs the ability to impose conditions, including conditions relating to the use of entities in the supply chain, or require a C/NCSP to take specific action would help to mitigate identified risks with a proposed change.

48. Amending the Act to include a formal mechanism that requires the C/NCSP to continue to engage with Home Affairs after conditions or mitigations have been imposed, would ensure the conditions or mitigations have been implemented and are appropriate for the lifecycle of the change. In addition, it would ensure that the C/NCSP engages with Home Affairs should there be a significant change to the risk profile.

Security Capability Plans

49. Section 314C of the Act allows a C/NCSP to provide a Security Capability Plan to the CAC in any 12-month period to notify one or more proposed changes as an alternative to notifying the CAC of each change individually.

50. A Security Capability Plan may include the following elements:

- details of one or more notifiable changes the C/NCSP proposes to implement that may have a material adverse effect on the capacity of the carrier or carriage service provider to comply with its security obligations;
- a timeline setting out the when the C/NCSP proposes to implement each of the changes;
- details of the C/NCSP's practices, policies or strategies to comply with the security obligation;
- details of the measures the C/NCSP is implementing, or proposing to implement, to mitigate the risk of unauthorised interference with, or unauthorised access to, telecommunications networks or facilities; and/or
- any other information the C/NCSP believes is relevant to assessment of the proposed changes.

51. A Security Capability Plan does not require the following information:

- the steps taken over the previous year to meet the baseline security requirements;
- measures over the next year to ensure continued compliance;
- incidents experienced over the previous year; and
- steps taken to remediate and address vulnerabilities.

Sector response to Security Capability Plans

52. Similar to individual notifications, C/NCSPs have conveyed concerns to Home Affairs that lodging a Security Capability Plan may be viewed as an admission that the C/NCSP is proposing to breach its security obligation or to do an act that is prejudicial to security.

53. Despite being included in the TSSR regime as a result of industry feedback, engagement with the telecommunications sector has indicated that C/NCSPs do not see the merit in submitting a Security Capability Plan and to date, the CAC has not received any Security Capability Plans since the commencement of TSSR.

Potential enhancements

54. One approach may be to require C/NCSPs to have in place a security capability plan that demonstrates how they are meeting their baseline security requirements and that can be updated from time to time. However, the proposed amendments to SOCI Act will require captured critical infrastructure entities to put in place a risk management plan which would take an all hazards approach and are therefore likely to encompass all of the requirements under the current security capability plan provisions. Noting that

telecommunications remains a key sector of critical infrastructure, the PSO, if applied to the telecommunications sector as it is currently proposed for the other sectors outlined in the draft Security Legislation Amendment (Critical Infrastructure) Bill 2020, could replace the current security capability plan provision. Should Government decide not to apply the PSO to the telecommunications sector, the current security capability plan provisions, while not being used by industry thus far, remain an option to be used for the convenience of industry to minimise the number of separate notifications they may be required to submit.

Directions power

55. Section 315A of the Act allows the Minister for Home Affairs to issue a written direction to a C/CSP not to use or supply, or to cease using or supplying, a carriage service if, after consulting the Prime Minister and the Minister for Communications, Cyber Safety and the Arts (being the Minister who administers the Act), the Minister for Home Affairs considers the proposed use or supply of the carriage service is or would be prejudicial to security.

56. Section 315B within the Act allows the Minister for Home Affairs, subject to safeguards, to direct a C/CSP or CSI to do or not do a specific act or thing to reduce or eliminate a national security risk.

57. Both powers are considered to be a measure of last resort where the continued operation of the carriage service would give rise to such serious consequences that the entire service would need to cease operation, or in the case of a Direction issued under 315B of the Act, to enable other action to be taken to address a security risk where the circumstances do not require the complete shut-down of the carriage service. To date, these powers have not been exercised.

58. The Minister for Home Affairs can only issue a s315B Direction if the Minister is satisfied there is a risk of unauthorised access to networks or facilities that would be prejudicial to security within the meaning of the ASIO Act and ASIO has issued an Adverse Security Assessment (ASA) in relation to the C/CSP or CSI. In addition, the Minister may only issue a s315B Direction if satisfied that all reasonable steps have been taken to negotiate in good faith with the C/CSP to achieve an outcome of eliminating or reducing the security risk.

59. A security assessment is an important administrative process that is subject to natural justice principles and, if the security assessment is one to which Part IV of the ASIO Act applies, may be reviewed in the Administrative Appeals Tribunal.

Addressing national security risks

60. The lengthy administrative process to seek a Direction could prevent the timely management of national security risks. For example, should a threat materialise from certain carriers that requires immediate action by Home Affairs, the Directions power cannot be relied upon quickly to enforce any required action.

61. Home Affairs is aware that there could be instances where the national security risk does not emanate from the C/CSP or CSI, but rather from the actions of an entity in the C/CSP's or CSI's supply chain. Under the current legislation, a Direction can only be issued on a C/CSP or CSI.

Potential enhancements

62. The Directions powers are considered to be appropriate last resort mechanisms. However, the graduated powers that will be available under the CI/SONS reforms, should they be passed by Parliament, would assist to provide options for Government to address risks that are of a lower order in sectors covered by the draft Security Legislation Amendment (Critical Infrastructure) Bill 2020 and ultimately in the telecommunications sector if they were extended to that sector. In particular, graduated powers being designed under the CI/SONS reforms could extend the positive security obligation that includes risk management planning obligations which would allow Government to indicate where telecommunications entities may need to take steps to address risks in their supply chains without resorting to the Directions power.

Information gathering power

63. Section 315C of the Act enables the Secretary of the Department of Home Affairs (or the Director-General of Security if authorised), to obtain information or documents from C/CSP/CSIs to assess their compliance with the security obligation.

64. This provision is necessary to ensure that Government can access any relevant information required to make an assessment regarding the C/CSP/CSIs compliance with its security obligation, which in turn informs the risk to national security. To ensure the relevant information is accessible, this power removes the privilege against self-incrimination, meaning a C/CSP/CSI cannot refuse to comply with a request for information on the grounds that the information may incriminate the person or expose the person to a penalty.

65. This power can only be delegated to the Director-General of Security and cannot be delegated to appropriate SES officers.

66. To date, this power has not been exercised as any information requested by Home Affairs has been provided voluntarily due to the good faith relationships it has with C/CSPs. However, in situations where good faith relationships cannot be relied upon, there is some doubt as to whether this power would achieve the desired security outcome as the power can only be used to confirm whether or not there is non-compliance with the security obligation.

67. Where the C/CSP/CSI has responded to the request for information, the framework is silent about the Secretary or Delegate being able to advise the C/CSP/CSI of any identified risks associated with their compliance with their security obligation and is unable to suggest any mitigations to address these risks. The Secretary or Delegate is unable to enforce any mitigations as a result of assessing a C/CSP/CSI's compliance with the security obligation. Additionally, there is no formal mechanism to acknowledge satisfaction with a C/CSP/CSI's compliance with their security obligation.

Potential enhancements

68. The information gathering power within TSSR could be enhanced by aligning it with the SOCI Act which allows the Secretary of the Department of Home Affairs to delegate this power to an SES employee. The information gathering power could be enhanced by allowing the Secretary or Delegate to take action in response to assessing the information provided by the C/CSP/CSI. For example:

- advise the C/CSP/CSI that risks have been identified;
- enforcement of conditions or mitigations to address the identified risks; or
- acknowledge satisfaction of compliance with the security obligation.

Engagement and information sharing

69. Australia's telecommunications sector is diverse in nature with broad and unique customer bases and service offerings. As of November 2020, there are 318 active licenced carriers in Australia.

70. There are other entities who may not fall under the legislative definitions for carriers or carriage service providers (C/CSPs) and so are not regulated by TSSR, but nonetheless maintain a high level of access to sensitive telecommunications infrastructure and data. These entities include: over-the-top (OTT) service providers (access to data only), cloud service providers, systems integrators, submarine cable operators and associated vendors, space sector companies, managed service providers, and data centre operators. In addition, vendors and equipment manufacturers are not regulated by TSSR, and C/CSPs are not required to disclose their vendors unless in the context of a notification assessment or use of the information gathering power.

71. Home Affairs engages with carriers relative to the extent and criticality of the infrastructure they own and operate, and the volume of telecommunications traffic and customers reliant on these carriers' infrastructure. Home Affairs is also currently engaged in an extensive outreach program with smaller C/CSPs to bring their attention to the TSSR regime and ensure they are aware of relevant risks to their networks.

72. Home Affairs continues to engage with C/CSPs on a case by case basis to provide in-depth technical guidance and targeted security assistance to carriers outside the formal notification process. Home Affairs uses these opportunities to discuss potential risks and provide guidance on designing and implementing targeted mitigations.

73. TSSR remains a key mechanism for, and has enhanced, formal and informal engagement between Home Affairs and the telecommunications sector to provide clarity around Government's expectations on managing national security telecommunications risks while allowing the sector the necessary flexibility to find the most appropriate and innovative solutions. However, under the current legislated framework, the onus for engaging with Home Affairs for notification obligations remain with the C/NCSPs.

74. More broadly, Home Affairs maintains engagement with the telecommunications sector through the Communications Sector Group of the Trusted Information Sharing Network and through close collaboration with the Department of Infrastructure, Transport, Regional Development and Communications.

Guidance materials

75. Home Affairs has developed a dedicated website with a secure portal for the telecommunications sector to submit notifications and enquiries. A range of guidance materials has been developed in consultation with the telecommunications sector to assist the sector to understand their obligations, including the TSSR Administrative Guidelines, fact sheets, Frequently Asked Questions and examples of the type of changes to networks and systems that may trigger a notification. These guidance materials are intended to inform the sector of Home Affairs' expectations of how the current regulatory framework should be interpreted and applied. They are also intended to provide industry with feedback about the types of security concerns they should be focusing on to improve the security of telecommunications networks.

76. As part of its extensive outreach program, Home Affairs has sought industry feedback on the guidance materials provided on the website. Feedback was generally positive, but industry expressed a desire for more precise language and specific direction about expectations. As a result, the TSSR Administrative Guidelines were updated on 5 November 2020.

APPENDIX A

Availability	Availability is about ensuring that authorised users have access to information, communications and telecommunications networks and facilities when required.
Carrier	A carrier is defined in the *Telecommunications Act 1997* to mean the holder of a carrier licence.
Carriage service provider	A carrier service provider (CSP) is defined by the *Telecommunications Act 1997* to be a person who supplies, or proposes to supply, a listed carriage service to the public using: • a network unit owned by one of more carriers, or • a network unit in relation to which a nominated carrier declaration is in force. A CSP may include an international CSP, a secondary user of an exempt network unit, an intermediary and a specified person declared by the Minister as a CSP.
Carriage service intermediary	A carriage service intermediary (CSI) is defined in the *Telecommunications Act 1997* as a person who is a carriage service provider under subsection 87(5) of that Act.
Communications Access Co-ordinator	The Communications Access Co-ordinator (CAC) is a role established under section 6R of the *Telecommunications (Interception and Access) Act 1979 and performed* in the Department of Home Affairs.
Confidentiality	Confidentiality under 313 (1A) and (2A) of the *Telecommunications Act 1997* relates to the obligations to protect information and communication from unauthorised access or unauthorised interference for the purpose of security.
Integrity	Integrity relates to the accuracy and completeness of information and communications, as well as the protection of telecommunications networks and facilities from compromise or unauthorised modification.
Nominated carriage service provider	A carriage service provider covered by a declaration in force under subsection 197(4) of the *Telecommunications (Interception and Access) Act 1979.*
Security	Section 4 *of the Australian Security Intelligence Organisation Act 1979* provides that **security** means: (a) the protection of, and of the people of, the Commonwealth and the several States and Territories from: (i) espionage; (ii) sabotage; (iii) politically motivated violence; (iv) promotion of communal violence; (v) attacks on Australia's defence system; or (vi) acts of foreign interference; whether directed from, or committed within, Australia or not; and (aa) the protection of Australia's territorial and border integrity from serious threats; and (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).
Telecommunications service	Telecommunications service is defined in the *Telecommunications (Interception and Access) Act 1979* as a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system

	operated by a carrier but not being a service for carrying communications solely by means of radio communication.
Telecommunications system	Telecommunications system is defined in the *Telecommunications (Interception and Access) Act 1979* as (a) a telecommunications network that is within Australia; or (b) a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia; and includes equipment, a line or other facility that is connected to such a network and is within Australia.