CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

SUBMISSION TO THE PJCIS:

REVIEW OF THE TELECOMMUNICATIONS SECTOR SECURITY REFORMS

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: Review of Part 14 of the *Telecommunications Act 1997* - Telecommunications Sector Security Reforms

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of Part 14 of the *Telecommunications Act 1997* - Telecommunications Sector Security Reforms (the Act) (TSSR).

About the Cyber Security Cooperative Research Centre

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has three research programs: Critical Infrastructure Security, Cyber Security as a Service, and Law and Policy.

The CSCRC is a public company limited by guarantee and will invest $AU50 million of Australian Commonwealth Government funding, and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas. The CSCRC has 25 Participants including seven Research Providers, eight State and Federal Government Agencies/Departments and 10 Industry/SMEs.

The TSSR review

The CSCRC recognises that the protection of telecommunications infrastructure and the information it transmits from espionage, sabotage and foreign interference is in Australia's national interest. Hence, the CSCRC supports fair and proportionate measures that help ensure Australia's networks and communications infrastructure are adequately secured, guided by a clear regulatory framework. The TSSR has established such a framework and, as illustrated during its two years of operation, has been adopted by industry and strongly supported with guidance and advice from government. Importantly, it is a key element in

bolstering national security, helping ensure Australia remains a safe and prosperous nation and trusted place to do business.

To this end, the CSCRC contends that:

- The application of the TSSR has been proportionate, noting the extraordinary powers of the Minister and Secretary for Home Affairs have not been used.
- The Department of Home Affairs has played a collaborative and helpful role in assisting carriers meet their TSSR obligations.
- The definition of 'security' is sufficiently broad to remain fit-for-purpose in the context of TSSR, capturing the evolving and constantly changing security threat landscape.
- Supply chain integrity is vital to ensuring the security of Australia's C/CSPs.
- Every reasonable step must be taken to ensure C/CSPs are not compromised – and that includes evaluating and preventing risks associated with companies providing 5G technologies.
- Acute attention must be paid to MSPs operating on behalf of C/CSPs.

The CSCRC looks forward to answering any queries the PJCIS has regarding this submission and welcomes the opportunity to participate in future discussions on this very important matter.

Yours faithfully,

Rachael Falk, CEO, CSCRC

ceo@cybersecuritycrc.org.au

Key elements of the TSSR and its application since introduction

The TSSR, which came into effect on 18 September 2018, was introduced to establish a regulatory framework to help mitigate and manage the national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities.[1] It comprises four key elements:[2]

- **Security obligation:** All carriers, carriage service providers and carriage service intermediaries (C/CSPs) must do their best to protect networks and facilities from unauthorised access and interference. This includes a requirement to maintain 'competent supervision' and 'effective control' over networks and facilities.
- **Notification requirement:** C/CSPs must notify the government of proposed changes to their networks and services that could compromise their ability to comply with their security obligations.
- **Information gathering power:** The Secretary of the Department of Home Affairs (the Department) can obtain information from C/CSPs and intermediaries to monitor and investigate their compliance with security obligations.
- **Directions power:** The Minister for Home Affairs has the power to direct a C/CSP or intermediary to do, or not do, a specified thing that is reasonably necessary to protect networks and facilities from national security risks.

During its operation (to 30 June 2020), the Minister for Home Affairs has not used the directions powers afforded under the TSSR regime, nor did the Home Affairs Secretary utilise information-gathering powers.[3] [4] Over this period, 66 notifications of change were received, 34 in the 2018-19 reporting year,[5] and 32 in the 2109-2020 reporting year.[6] The CSCRC contends the application of the TSSR has, during its relatively short operation, been proportionate, noting the extraordinary powers of the Minister and Secretary for Home Affairs have not been used. Furthermore, the CSCRC commends the Department for the collaborative and helpful role it has played in enabling C/CSPs to meet their obligations under the Act. This clearly illustrates the Department's objective "to achieve national

[1] https://www.homeaffairs.gov.au/nat-security/Pages/telecommunications-sector-security-reforms.aspx
[2] https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/telecommunications-sector-security-reforms

[3] https://www.homeaffairs.gov.au/nat-security/files/tssr-annual-report-2018-19.pdf
[4] https://www.homeaffairs.gov.au/nat-security/files/tssr-annual-report-2019-20.pdf
[5] https://www.homeaffairs.gov.au/nat-security/files/tssr-annual-report-2018-19.pdf
[6] https://www.homeaffairs.gov.au/nat-security/files/tssr-annual-report-2019-20.pdf

security outcomes on a cooperative basis rather than through the formal exercise of regulatory powers".[7]

The definition of security

For the purposes of the Act, the ASIO Act[8] definition of 'security' is applied, which includes the protection of the Commonwealth, states, territories and the people of Australia from espionage, sabotage, attacks on Australia's defence system and acts of foreign interference. In addition, it comprises the protection of Australia's territorial and border integrity from serious threats and the carrying out of Australia's responsibilities to any foreign country in relation to protecting Australia's territorial and border integrity from serious threats. Such a definition is sufficiently broad to remain fit-for-purpose in the context of TSSR, capturing the evolving and constantly changing security threat landscape.

As noted in the Explanatory Memorandum,[9] C/CSPs are attractive targets for espionage, sabotage and foreign interference. They can be impacted through the compromise or degradation of telecommunications networks; compromise of valuable data or information of a sensitive nature; and impairment of the availability or integrity of telecommunications networks. In the event compromise does occur, the impact is felt much more broadly due to the reliance on C/CSPs by government services and other critical infrastructure entities.

Supply chains and *The Modern Slavery Act 2018*

Undoubtedly, C/CSPs are vulnerable to espionage, sabotage and interference activity, with a key risk factor being the supply of equipment, services and support arrangements[10] sourced via global supply chains. Additionally, the rapid pace of technological advances has also created new and complex vulnerabilities to C/CSPs, which include the ability to disrupt, destroy or alter networks and their critical infrastructure, and to compromise information on these networks. For this reason, supplier and supply chain integrity are vital to ensuring the security of Australia's C/CSPs.

---

[7] https://www.homeaffairs.gov.au/nat-security/files/tssr-annual-report-2019-20.pdf
[8] https://www.legislation.gov.au/Details/C2019C00024
[9] Explanatory Memorandum, *Telecommunications and other Legislation Amendment Bill 2016*, Parliament of the Commonwealth of Australia, pp 2-3.
[10] Explanatory Memorandum, *Telecommunications and other Legislation Amendment Bill 2016*, Parliament of the Commonwealth of Australia, pp 2-3.

The CSCRC strongly believes that shoring up the security of critical technology supply chains is essential to ensuring Australia's future prosperity and reputation as a safe and trusted place to do business, and supports the introduction of the draft *Critical Technology Supply Chain Principles*, which were recently released for discussion by the Department. In its *Mobile Telecommunications Security Threat Landscape*[11] report, the GSMA notes that "attackers do not need to compromise their intended target directly but in many cases can achieve their aim by compromising the supply chain where it is least secure". The report cites several examples including chip tampering[12] and mobile phones with in-built vulnerabilities being sold in the US market.[13]

This potential threat highlights the importance of managing the supply chain holistically and driving out or mitigating insecure elements. Hence, the provisions of Australia's *Modern Slavery Act 2018*[14] (the MS Act) are vital for national security, as they provide thorough oversight into the human capital and geographical components of goods and services flowing into the Australian market, which could potentially be compromised. The MS Act encourages businesses to take a technology-led approach to monitoring supply chains, providing rigorous and largely incorruptible visibility into these supply chains. This helps provide assurance that the goods and services C/CSPs use within their supply chains do not present a national security risk. In its current form, the MS Act only applies to large businesses and entities in the Australian market with a consolidated revenue of at least $100m. These businesses are required to prepare annual modern slavery statements, which identify and mitigate modern slavery risks in their global operations and supply chains. The CSCRC submits that this threshold could be lowered to capture businesses and entities with a consolidated revenue of $50m. Such a move would capture a broader cross-section of Australian businesses or global entities operating within Australia and, as a result, more threats to C/CSP supply chains could be detected.

TSSR and 5G

The advent of 5G has, and will continue to, vastly alter the environment in which C/CSPs operate within and the security standards they must maintain. And there is no doubt the implementation of 5G networks will have a profound influence on geopolitics moving

[11] https://www.gsma.com/security/wp-content/uploads/2019/03/GSMA-Security-Threat-Landscape-31.1.19.pdf, p 5.
[12] https://www.computing.co.uk/news/3060992/security-researcher-claims-via-c3-x86-cpus-contain-hidden-god-mode
[13] https://www.wired.com/story/android-smartphones-vulnerable-out-of-the-box/
[14] https://www.legislation.gov.au/Details/C2018A00153

forward because a threat anywhere in the network will be a threat to the whole network. In 2018, the Federal Government banned high-risk vendors from providing 5G technology for wireless networks due to national security concerns.[15] Central to this decision was the threat of disruption to a network as a result of third-party interference, which could cripple business, supply chains and other critical infrastructure Australians rely on. Earlier this year, the Australian Signals Directorate's former head of signals intelligence and offensive cyber missions, Simeon Gilding, poignantly observed: "Cyber security is all about raising the costs for the attacker. Network access through vendors—which need to be all over 5G networks to maintain their equipment—effectively reduces the access cost to zero".[16] The CSCRC supports the notion that every reasonable step must be taken by C/CSPs to ensure these systems are not compromised – and that includes evaluating and mitigating potential risks associated with companies providing 5G technologies.

The CSCRC notes that in its recent report, *The Next Gen Future*, the House of Representatives Standing Committee on Communications and the Arts identified security of the 5G network from "design to implementation and maintenance"[17] as a key priority. Of particular importance were concerns raised about the convergence of mobile and fixed line networks and the potential security vulnerabilities that could arise, with Palo Alto submitting that "detection and prevention is the key ingredient to the infrastructure".[18] The CSCRC agrees with recommendations that real-time visibility of traffic passing through 5G networks is vital to identifying and mitigating cyber security threats, with development of effective automation, artificial intelligence and machine learning technologies essential to security uplift.

Managed Service Providers (MSPs)

The CSCRC notes that in the TSSR 2019 Annual Report, the Department highlighted an increasing number of notifications involving managed service providers (MSPs), as well as an increase in the range and scope of functions it was proposed these MSPs should undertake.[19] In the CSCRC's opinion, the Department was right in raising concerns about both the ability of C/CSPs to maintain adequate supervision over MSPs and in effect, ensure

15 https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/6164495/upload_binary/6164495.pdf;fileType=application%2Fpdf#search=%22media/pressrel/6164495%22
16 https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/
17 Parliament of the Commonwealth of Australia, *The Next Gen Future*, March 2020, p 27.
18 Parliament of the Commonwealth of Australia, *The Next Gen Future*, March 2020, p 28.
19 https://www.homeaffairs.gov.au/nat-security/files/tssr-annual-report-2019-20.pdf

the integrity of networks and infrastructure, and the lack of consideration as to where MSPs would be operating from (e.g. overseas locations).[20] Such concerns are not unfounded, with the case of Operation Cloud Hopper setting clear precedent as to why MSPs must be carefully vetted and regulated and why such a requirement must be clearly communicated to C/CSPs.

Operation Cloud Hopper was one of the largest ever sustained global cyber espionage campaigns,[21] which saw China's cyber espionage group, APT10, target IT MSPs, gaining access to sensitive intellectual property, intelligence and corporate and personal data. It is believed the group was operating in this capacity for approximately 10 years before being uncovered in 2016.[22] Operation Cloud Hopper impacted, among other organisations, NASA and 45 US tech giants,[23] and at least 12 countries, including Australia.[24]

The Australian Cyber Security Centre's 2018 investigation report, *Compromise of an Australian company via their Managed Service Provider*, details a computer compromise on the Australian arm of a multinational construction services company via an MSP, which was reported in March 2017.[25] The computer was compromised with specific malware that was previously publicly attributed to APT10.[26] As a result of the breach, which had been initiated in 2016, all corporate user and computer account details, including encrypted passwords were stolen.[27] There is no doubt such breaches have the potential to pose a serious threat to national security and acute attention must be paid to MSPs operating on behalf of C/CSPs.

Conclusion

There is no doubt the protection of telecommunications infrastructure and the information it transmits from espionage, sabotage and foreign interference is a matter of national importance. To this end, the CSCRC concludes the TSSR regime has established a fair and proportionate framework through which national security risks to Australia's networks and communications infrastructure can be mitigated.

---

[20] https://www.homeaffairs.gov.au/nat-security/files/tssr-annual-report-2019-20.pdf
[21] https://www.pwc.com.au/cyber/operation-cloud-hopper.html
[22] https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
[23] https://www.fbi.gov/wanted/cyber/apt-10-group
[24] https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
[25] https://www.cyber.gov.au/sites/default/files/2019-03/msp_investigation_report.pdf
[26] https://www.cyber.gov.au/sites/default/files/2019-03/msp_investigation_report.pdf, p 2
[27] https://www.cyber.gov.au/sites/default/files/2019-03/msp_investigation_report.pdf, p 4