Huawei Australia submission to the

Parliamentary Joint Committee on Intelligence and Security

Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms

27 November 2020

Introduction

1. As one of a handful of corporations to be negatively targeted by the Telecommunications Sector Security Reforms (TSSR) legislation, Huawei is well placed to provide first-hand experience of the implementation and impact of the legislation.

2. In fact, the application of the TSSR legislation on Huawei has led to the loss of 900 direct jobs, over 1500 sub-contracting jobs and over $100 million in research and development (R&D) investment in Australia.

3. Huawei Technologies Australia is a privately owned Australian-based company and there is no question our duties and obligations are to comply with Australian laws, including the TSSR. Furthermore, Huawei Australia's parent company is free of state ownership and owned 100 per cent by staff.

4. Huawei strongly supported the development of the TSSR legislation as it promised to provide clear security guidance for telecommunications operators and vendors. It promised to provide a transparent and open security framework to guide operators and vendors to develop products and networks that would meet Australian Government requirements and standards.

5. The reforms were touted as *'important to ensure the security and resilience of Australia's telecommunications infrastructure, as well as the social and economic wellbeing of our nation.'*[1] Unfortunately this has not eventuated. But it is not too late.

6. In this submission Huawei outlines future measures that can secure an open and competitive telecommunications market for Australia that is safe but also enables a long term approach to Cyber Security that means Australia doesn't have to continue to just say "no" to the world best technology because it is from a Chinese company like Huawei. There are many more Huawei's to come.

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

Executive Summary

7. In practice the TSSR legislation destroyed Australia's global mobile network leadership, reduced vendor competition, forced up prices for operators and consumers, isolated Australia from the world's leading 5G innovation (as well as the ongoing leading innovation in 6G, 7G etc) and failed to make the nation any safer.

8. The TSSR reforms could be viewed as a tool designed to remove Huawei and other Chinese headquartered companies from the market. TSSR hasn't made the Australian telecommunications network any safer or more secure. In fact, we argue because of the overdependence on one single vendor in Australia the security risk of a 'single point of failure' has made Australia's telecom networks far more vulnerable.

9. Despite banning Chinese companies like Huawei from providing 5G technology in Australia, all the 5G equipment installed on the 5G networks today is still made in China with companies part-owned by the Chinese Government and without any independent security testing or evaluation. (see Attachment 1 from XenophonDavis for more detailed information)

10. Australia now has a virtual 5G vendor monopoly situation, resulting in: increased costs for operators resulting in delays and restrictions to the 5G roll out and more expensive plans for consumers. Regional Australia will wear the brunt of the Huawei ban as the business case to deploy 5G in more rural and provincial areas is more difficult to support.

11. Chinese companies (vendors) are banned from selling 5G technology but all of Australia's current 5G equipment is being made in China in partnership with Chinese Government owned companies. If the 'risk' is China, then how is it that Ericsson and Nokia can still manufacture, compile software and work in partnership with the Chinese government for building 5G technology and then deliver those products into the Australian 5G networks with no independent testing?

12. Huawei believes Australia should implement a policy that enables independent testing and verification of ALL vendors' technology. Huawei has nothing to hide, and has always advocated for a universal testing regime for everyone. We are the only vendor in Australia that supports such independent testing. We have continued to try and gain industry wide support for such a policy (as there is in the EU) but so far we have been blocked by the other vendors. Ironically the parent companies of these vendors support such a policy in the EU.

13. The Turnbull Government relied on the wrong network architecture and technology advice to ban Huawei (and other Chinese vendors) from 5G. The advice given to the Turnbull Government has been totally refuted by the global industry standards association that manages the regulations of 5G, the UK Government and the telecommunications operators.

14. Australia missed the opportunity to become a regional security testing and assurance hub for 5G and 6G, 7G etc by establishing an open and transparent security framework that works with all vendors and implements global best practice for the onslaught of next generation technology that will emerge from China for decades. The Turnbull Government's policy of just saying 'no' was short sighted.

15. The fundamental issues surrounding the banning of Huawei in 5G will not go away. There will be 6G and 7G. There will be new technologies and innovations like AI, quantum computing, robotics and many more coming from Chinese companies like Huawei. A lot of these companies will be the world leaders in what they do, like Huawei is in 5G. Is the future policy under TSSR to just say no to them all? Can Australia really afford that?

Background

16. Huawei was a welcome and active participant in the consultation process to formulate the TSSR legislation. As the world leading telecommunications vendor Huawei has enormous expertise building safe and secure networks around the world. We work with operators in over 170 countries around the world to develop and build the networks to best serve their people.

17. Huawei tendered a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) *Inquiry into potential reforms of Australia's national security legislation* and former Huawei Chairman, Mr John Lord AM and Managing Director, Mr David Wang followed up with an appearance at a Public Hearing on 14 September 2012. In the following years Huawei provided regular written and in-person advice to the Attorney General's department and contributed to the *Communications Alliance* response to the consultation process.

18. The premise of the TSSR was welcomed by Huawei as the certainty of clear and concise security policy would provide our customers with the clarity they needed to deploy Huawei products safely and securely in their Australian networks - just as they have done for over a decade.

19. In fact, in a letter to the then Huawei CEO, Mr James Zhao (Attachment 1) in August 2015, former Communications Minister, the Hon Malcolm Turnbull MP was very clear that the TSSR would not seek to ban vendors from supplying services or equipment to the Australian telecommunications market (Attachment 2):

> *I can assure you that the obligations under TSSR do not apply to suppliers and do not seek to exclude any specific supplier from offering services or equipment to the Australian telecommunications market. It is regrettable that recent media attention has led to questions from current and potential customers regarding your products and services.*
>
> The Hon Malcolm Turnbull, Minister for Communications
> Letter to Huawei Australia Chairman, August 11, 2015

20. On 23 August 2018, one month before the TSSR legislation was enacted, it was cited in the Australian Government press release effectively banning Huawei from 5G.[2]

21. Huawei was banned in the chaotic hours before Prime Minister Malcolm Turnbull was removed as Liberal leader. Huawei's treatment was disappointing considering the important role we played in building critical 3G and 4G mobile networks in Australia for over 15 years.

22. Huawei Chairman Mr John Lord was called by then Secretary of the Department for Communications and the Arts, Mr Michael Mrdak five minutes before the press release was issued to ban the company without any reason other than Huawei was a Chinese headquartered company. The public press release, which doesn't mention Huawei or China, remains the only written notification of the ban Huawei has had.

23. In 2020, the former Prime Minister Mr Turnbull confirmed in his book *A Bigger Picture* that there was no 'smoking gun' and Huawei was banned as a 'hedge'.

24. Instead of using the legislation - which Huawei supported – to develop a highly competitive, cost effective, more innovative and secure telecommunications environment, Australia chose an inconsistent approach bereft of evidence and transparency that has

[2] https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F6164495%22

isolated businesses and consumers from the world's best 5G equipment.

25. The TSSR legislation did not provide Huawei with any formal notification or reasons for the ban. Our equipment was never tested and Government officials never accepted repeated offers to inspect our manufacturing plants and review our cyber security processes. Nine years on from the NBN ban and two years on from the 5G ban Huawei does not know why the bans have been put in place and have still not received any formal notification about either of the bans.

26. Within the August 2018 press release announcing the ban, the Turnbull Government highlighted two reasons for the decision:
    - an assumption that it was not possible to split the Core and Non-Core (Edge) of a 5G network; and
    - the possible influence by a foreign government on certain vendors.

27. Huawei disputes both reasons cited in the press release.

28. **Ability to Split between Core & Non-Core (Edge) in 5G**

    The Government suggested 5G would be configured differently to 4G and posed a greater network security risk. The security advice inaccurately declared that Core and Non-core (Radio Access Network (RAN)) parts of new 5G networks could not be separated. The split can be clearly demonstrated in 5G networks around the world where Huawei supplies the RAN but another vendor suppliers the core.

29. The global telecommunications industry also dismisses the Australian Government reasoning. The global 5G standards agencies 3GPP and GSMA, the vendors that make the technology and the global operators that run the 5G networks clearly state that Core and Non-Core parts of the network are similar to current 4G networks.[3]

30. In fact, a UK Parliamentary Committee concluded that the Australian position was contrary to **all** the evidence they gathered. In truth, 5G network architecture is very similar to the 3G and 4G networks that Huawei has deployed in Australia over the past 15 years.

31. Two UK Parliamentary Committees concluded that there were "no technical reasons" why Huawei should be banned from supplying 5G technology in the UK. (Huawei currently supplies around 60% of the UK's 5G RAN technology across all four telecom operators, EE, Vodafone, O2 & Three UK).

32. The UK Parliamentary Committee on Science and Technology said:

    "Although the Australian Government has concluded that the distinction between Core and Non-Core networks will be less clear than for previous technology generations, we heard unanimously and clearly that a distinction between the Core and Non-Core parts will still exist."[4]

33. The **UK Intelligence and Security Committee** went further and said banning one vendor would actually make the UK 5G networks less secure:

    "…the telecommunications market has been consolidated down to just a few players: in the case of 5G there are only three potential suppliers to the UK – Nokia, Ericsson and Huawei. Limiting the field to just two…would increase over-dependence and reduce competition, resulting in less resilience and lower security standards. Therefore including a third company – even if you may have some security concerns about them and will have

[3] http://huaweihub.com.au/the-facts-on-5g/

[4] https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/190710-Chair-to-Jeremy-Wright-re-Huawei.pdf

to set a higher a bar for security measures within the system – will, counter-intuitively, result in higher overall security." [5]

34. In January, after thorough investigation and scrutiny the UK Government initially cleared Huawei to deploy 5G network equipment. In June, under intense pressure from the US Government the UK Government back-flipped on its original decision and will only permit Huawei 5G equipment to operate in UK networks until 2027.[6]

35. The UK backflip was not accredited to any Huawei wrongdoing, 5G network architecture or perceived Chinese influence but rather a concern US Government policy changes to block Huawei's access to American made semi-conductors and chipsets could lead to 'less trustworthy' network equipment.[7]

36. As a global technology provider, Huawei is acutely aware of just how important cyber security is for ensuring trust in the digital world we all share. The aviation industry has developed clear and consistent security and operational policies and protocols to allow flights to crisscross the world, largely without incident. It's time the telecommunications and IT industries did the same.

37. Huawei has consistently called for independent and robust cyber security evaluation, assessment and testing for every vendor's equipment under the TSSR. Unfortunately, our competitors in Australia continue to resist additional security measures and scrutiny to protect local networks. Working closely with the Australian telecommunications industry peak body Communications Alliance to prepare a response to recently proposed national cyber security policy, Huawei's suggestion to develop tougher and more stringent cyber security policy was rejected by our competitors.

38. **Potential for Foreign interference and Chinese laws**

    If the potential influence of the Chinese Government is the reason for blocking Huawei from Australia's 5G build, then such a ban should be considered for our competitors. The 5G equipment being installed by Nokia and Ericsson in the Telstra, Optus and Vodafone networks is made in joint-venture operations that are part owned by companies that are ultimately owned by the Chinese Government.[8]

39. In fact the TSSR legislation permits Telstra and Optus to install 5G equipment made in China by the Ericsson/Panda Electronics joint venture, while the US Department of Defense has listed Panda Electronics as a company that is either owned by or controlled by the People's Liberation Army.[9]

40. Either the Australian Government did not know the alternative suppliers to Huawei both manufactured their 5G equipment in joint ventures with the Chinese Government or they do not believe they are subject to 'extra-judicial' influence – even when Chinese Government controlled companies run their factories.

41. Australia has presumed Nokia and Ericsson can be trusted because they are headquartered in countries that are close European allies: Huawei, conversely, cannot be trusted because it's headquartered in China.

[5] UK Intelligence and Security Committee 5G Report
[6] https://www.theguardian.com/technology/2020/jul/18/pressure-from-trump-led-to-5g-ban-britain-tells-huawei
[7] https://www.ncsc.gov.uk/blog-post/a-different-future-for-telecoms-in-the-uk
[8] https://telecomstechnews.com/news/2018/aug/13/nokia-ericsson-china-communist-party/
[9] https://www.axios.com/defense-department-chinese-military-linked-companies-856b9315-48d2-4aec-b932-97b8f29a4d40.html

42. We do not argue that the two Nordic companies are not worthy of trust in a traditional sense, but strongly urge that the determination that a company is worthy of trust—and thus that its products should automatically be deemed trustworthy—should not depend solely on where the company is headquartered.

43. In recent years many high profile hacking incidents have been highlighted in Australia and around the world. In a significant number of these incidents attackers compromised the target systems through a trusted vendor. Trust that is not based on evidence is a network security design flaw.

44. Huawei is headquartered in Shenzhen but both Nokia and Ericsson develop many of their products in China and manufacture hardware there. Telstra and Optus 5G supplier, Ericsson operates five innovation centers in China including one focused on 5G. Nanjing is the company's largest manufacturing and logistics base worldwide and the location where Ericsson makes its 5G gear. Ericsson has 11,000 staff in China, roughly 5,000 of whom work in R&D.[10]

45. Similarly, TPG-Vodafone 5G supplier, Nokia co-owns its Chinese subsidiary, Nokia Shanghai Bell, together with a Chinese state-owned enterprise, China Huaxin, which holds just over 49 percent of the venture and has the right to nominate its CEO.[11] From 2002 to 2017, the unit's chairman also acted as the Secretary of the Chinese Communist Party committee within the company (every company of a certain size that does business in China is required to have a Party committee).

46. The TSSR allows Australian operators to deploy Nokia or Ericsson (or both), firms with substantial operations in China, and large numbers of Chinese personnel. Instead of making assumptions about trustworthiness based on where a company is headquartered, Huawei believes it is essential to focus on the assurance and transparency requirements and features of all the key players, including the telecom and mobile operators, on the one hand, and the equipment (and other third-party) suppliers, on the other.

47. Manufacturing in China is not a criticism of either of our competitors but reflects the reality of the telecom global supply chain. We all have similar supply footprints and as such it is impossible to place a flag of origin on any particular product. For example an Apple iPhone is designed in the USA, but the componentry comes from Japan, Taiwan, USA, China and Europe. It is then assembled in China (at the same factory that many Huawei phones are assembled). What is the country of origin of that product?

48. TSSR legislation focuses on the telecommunications operators and not the vendors and manufacturers that spend billions of dollars researching, developing standards, securing, building and deploying the equipment that it so important to Australian businesses and consumers. Telecom operators do not make the equipment and do not always have the global security expertise the vendors have acquired deploying around the world. Huawei invests AUD$30 billion a year to develop the advanced secure equipment that powers telecom networks globally and greater consideration of this knowledge and expertise is required under the legislation.

49. Currently under TSSR the relationship and engagement is with the operators not vendors. This doesn't enable the Australian government to get a full understanding of future technology as it is being developed and researched. Already Huawei (and others) R&D teams are well into 6G development, setting the requirements and functions for its roll-out. Now is the time to start conversations around security. It is the vendors that are

[10] https://www.ericsson.com/en/press-releases/2012/9/ericsson-inaugurates-new-rd-facilities-in-nanjing
[11] https://www.nokia.com/about-us/news/releases/2017/05/18/nokia-and-china-huaxin-sign-definitive-agreements-for-creation-of-new-nokia-shanghai-bell-joint-venture/

making these decisions and breakthroughs. TSSR doesn't make room for such relationships and knowledge transfer.

50. To be absolutely clear, despite numerous inaccurate reports in the media, Chinese law does not require Huawei to install 'backdoors' in networks or equipment. We have also independently verified this with leading Chinese law firm, Zhong Lun, and their view was reviewed and confirmed by Clifford Chance, one of the world's leading law firms. They confirmed that relevant provisions of the Counter espionage Law, the Anti-Terrorism Law, the Cyber Security Law, the National Intelligence Law and the State Security Law do not empower PRC government authorities to plant backdoors, eavesdropping devices or spyware in telecommunications equipment.

51. Huawei founder Mr Ren Zhengfei has confirmed he has never received such a request and would close down the business if asked. Huawei is an independent company and customer-centricity lies at the heart of all we do. Huawei would never compromise or harm any country, organisation or individual, especially when it comes to cyber security and user privacy protection. Huawei is the world's number one telecom vendor because global telecom operators trust our products and trust our staff. We have a proven track record over 30 years of delivering safe and secure technology across the globe. We would welcome the opportunity to provide all the benefits of our technology to Australia.

5G tax

52. The politicisation of the TSSR legislation has isolated Australia from the world's best technology and innovation, it will delay the rollout of future networks and curb competition forcing price hikes of 20-40% for operators and Australian consumers. This extra 5G deployment cost has already been confirmed by comments from executives at TPG, Vodafone and Optus.

53. One Australian carrier has advised Huawei it now costs 50 per cent more to build out a mobile base station site, forcing them to scale back their 5G targets.

54. A study by Frontier Economics[12] (Huawei-commissioned), found the cost to industry and Australian consumers of reduced competition from excluding Chinese vendors (Huawei) to be significant. They estimate the exclusion of Huawei will increase the cost of 5G radio access network (RAN) equipment in Australia by 18-42% for carriers, which will be recovered from consumers through higher retail prices. Further, for networks already using Huawei for 3G and 4G equipment, additional switching costs could add several billion dollars and materially delay 5G deployments. Telstra has already announced increases to mobile plans due to its 5G deployment of up to $15 per month.[13]

55. In the UK an independent report by respected research company Assembly Research estimated that the cost of excluding in effect Huawei from their 5G builds would cost the UK economy £6.8bn and delay the widespread establishment of 5G by 18-24months.[14]

56. Taking a broader look at the cost of excluding Huawei the GSMA (the global trade group for mobile operators) found that should Huawei be excluded from deploying 5G in Europe then the cost to operators would be some $AUD89 billion.[15]

---

12 https://www.frontier-economics.com.au/costs-of-excluding-huawei-from-5g-networks-in-australia/

13 https://www.dailymail.co.uk/news/article-8532053/Telstra-comes-fire-increasing-price-plans-5-people-struggle-make-ends-meet.html

14 https://www.mobileuk.org/supply-chain-security

15 https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3

57. Three different reports, from three respected authors all stating the same thing: reduce vendor competition and it will have an impact on prices and roll-out timelines of 5G.

58. Mobile consumers have had the unique situation over the past several years of a decrease in prices while enjoying an increase in service and coverage. This is about to change. Australia's restrictive 5G policy is effectively a '5G Tax' on the Australian telecommunications industry and consumers.

59. The Turnbull Government, unlike the UK Government, did not tell the business community or consumers of the overall cost on the Australian economy of the Huawei 5G ban. Without any Treasury modelling, Australian businesses and consumers are left in the dark to the total cost of the ban.

Regional

60. The financial business case for operators to build coverage in regional Australia will be difficult to near impossible because of the Huawei ban. A 30% increase in equipment costs will destroy what business case they currently have. We will see the Australian 5G footprint plans reduce considerably at the cost of regional Australia.

61. The restrictive Australian 5G ecosystem will also have an impact on the ability for Australian companies who are developing 5G applications (especially in agriculture & mining) to take their products to the global market. Huawei is and will remain the largest provider of 5G technology in the world. For example 60% of the current 5G Radio Access Network (RAN) equipment in the United Kingdom is Huawei. Australian companies developing 5G applications will not be able to test their products with the major global 5G technology player, restricting their opportunity to export to the world and holding back the local 5G ecosystem investment.

The Future - Securing an open and competitive telecommunications market

62. The TSSR must recognize global standards with conformance programmes to ensure that there is compliance. Vendors that cannot meet these requirements should be excluded. This will increase the demand for vendors who place a high value on security. Once determined what vendors must do, the Government must make that a requirement and have a programme in place to make sure they maintain compliance. Given the global nature of telecoms, there is also an opportunity for regulatory alignment with Europe and UK to sharpen the security incentives in these markets.

63. Measures to equalise cyber security standards across vendors should make it harder for a vendor to enjoy competitive advantage at the expense of security. Moreover, operators should be required to demonstrate to the Australian Communications and Media Authority and the Government that they have a comprehensive risk management and monitoring programme consistent with agreed-upon standards and other requirements, and that they have put in place appropriate architectural controls and other measures to address identified risks in their supply chain, regardless the country of origin of the deployed equipment.

64. Another critical way of improving TSSR should be through effective assurance testing and ongoing management of vendor equipment. Operators should work closely with vendors, supported by Australian Cyber Security Centre (ACSC), to ensure:
    a) A robust security development lifecycle process.
    b) Effective assurance in the context of that specific operator's deployment of designated equipment, systems and software.
    c) Ongoing verification arrangements to make sure that security requirements are met.

65. It is clear operators should prioritise greater security assurance and whole-of-life costing in their vendor base and the TSSR should help drive that. When taken together, these measures will create a robust and risk-based security regime for telecoms that will improve how the market works, without banning a carrier from accessing the best 5G technology. This new framework will allow the Government to respond to threats, risks and technology changes, including strengthening the controls if needed in the future.

66. Furthermore, the government should establish equivalent cyber security evaluation centres for all 5G equipment vendors in Australia, especially the ones supplying core networks.

67. In Australia, there is an industry need to create a more diverse and competitive supply base for telecoms networks. This will be critical to drive higher quality, innovation, reduce the risk of national dependency on individual suppliers, and attract more investments in the ICT field, especially on Cybersecurity.

68. Telecoms operators should be responsible for managing the risk and assuring the resilience of their networks, including the risk from equipment and other suppliers. Government should make sure the operators are managing their networks in conformance with regulatory requirements and industry best practices in a manner that provides assurance and transparency. Government should make clear to operators that they should not compromise appropriate risk management practices to achieve commercial priorities.

69. The business models of vendors should prioritise cyber security and privacy protection consistently with laws, regulations, standards, product certification requirements, and manage risk from suppliers. Moreover, the Government should demand for similar actions

from all vendors, as with Huawei Cyber Security Evaluation Centre (HCSEC) in the UK. All flaws resulting from practices that may have achieved good commercial outcomes but have resulted in poor cyber security should be identified in all equipment, regardless the label placed on them.

70. After input from the private sector, the TSSR should provide clarity to industry on what is expected in terms of appropriate risk management practices for network operators.

71. ACMA should engage industry to understand supply chain risks and the arrangements adopted by operators to mitigate them, and get regular updates on operators' major supplier arrangements and TSSR compliance plans.

72. As explained above, the current regulatory environment does not provide a risk assurance framework with a common understanding or methodology for identifying threats, assessing or managing risk, or promoting resilience. Nor have appropriate standards or best practices, or supporting conformance and testing protocols been developed, much less implemented, to facilitate ongoing assessment of the effectiveness of risk management and the state of network resilience. Specifically it does not provide guidance to address the fundamental questions to take the security of telecom networks extremely seriously in Australia, e.g.:
    a) How to incentivise telecoms operators to improve security standards and practices in their networks.
    b) How to address the security challenges posed by all vendors.
    c) How to create sustainable diversity in the telecoms supply chain.

73. The TSSR Act is in force with a ban on Huawei participating in 5G procurements. The Security of Critical Infrastructure Act (SCIA) is also in force with no clear directions on how to protect Gas, Water, Electricity and Ports infrastructures. The Assistance and Access (Decryption) Bill is also in force despite of the industry concerns, even making it very difficult for Australian based organisations to sell their cyber security services to the rest of the world.

74. Looking at mobile telecommunications infrastructure, currently, the TSSR (power of direction) makes the entire ICT infrastructure less secure by increasing the over-dependence from 1-2 vendors. It also makes the nation less prosperous by reducing competition and dis-incentivises investments in the ICT sector, especially on Cybersecurity.

75. Government needs to force the industry players to enhance governance, ICT infrastructure and device resilience, and incentivise them to properly manage their supply chain risk, in order to provide the requested level of assurance. For example, the TSSR should incentivise all vendors to address systemic engineering failures, as well as incentivise telecom operators to improve security standards and practices in 5G.

76. Also, incentives to inform the Government due to regulatory requirements (e.g. TSSR, SCIA) need to be in place to ensure carriers are not threatened by coming forward and asking for support from ASD to take the security of telecom networks extremely seriously in Australia, instead of prioritising their commercial interests.

77. Vendors should be subject to rigorous oversight through procurement and contract management. This involves operators requiring all their vendors to adhere to the existing legislation (TSSR; SCIA).

78. Operators must work closely with vendors, supported by Government, to ensure effective assurance testing for equipment, systems and software, and support ongoing verification arrangements. As done in Europe, the Government should define and mandate an Australian cybersecurity certification framework that enables the creation of tailored and

risk-based AU certification schemes.

79. TSSR should also ensure vendors and carriers build and operate secure and resilient networks, and manage their supply chains accordingly; and assess the risks posed by vendors, regardless of their country of origin, and apply proportionate and targeted controls to mitigate the risks, without banning operators and infrastructure owners from access to the best 5G technology. (Cyber supply chain includes the design, manufacture, delivery, deployment, support and decommissioning of equipment (hardware and software) or services that are utilised within an organisations cyber ecosystem. Supply chain must consider the whole lifecycle of an IT product or service in an organisation.)

80. The Government should be extremely cautious of making decisions solely based on nationality of a vendor. A vendor from a country whose laws are not likely contrary to Australian law, does lower the immediate elevation of risk associated with likely adverse extrajudicial control in nationally critical systems.

81. If the vendor is from a country of possible concern, and considered “high risk”, that alone should not rule out the vendor. Instead, consider the actual role of the system under question relative to critical data and perform risk assessment and mitigation through complimentary security controls.

82. Conversely, if a vendor is not from a country of concern with regard to extrajudicial influence, this should not immediately rule them as a lower risk option with regards to overall cyber supply chain risk. There are still cyber security vulnerabilities that must be considered and mitigated.

83. Ask vendors for evidence of compliance with commonly known standards they would already have to comply with for the different regions they operate in. In the absence of that, ask for demonstration that the vendor has complied with best practice guidelines and evaluate their products, regardless the country of origin.

84. Seriously consider actions to address and mitigate Cybersecurity concerns similar to what is ongoing in the EU, especially on the EU-wide Cybersecurity Certification schemes, and the policy response for a new robust security framework in the UK.

85. To strengthen cyber security the Government, in consultation with the industry, should consider:

    - A new set of network security and resilience requirements on 5G and fibre networks for telecoms operators, overseen by ACMA and Government, to design and manage their networks, as well as their business and governance processes, with higher standards and best practices. The adoption of the requirements by operators (and through them, suppliers) will mitigate network security and resilience risks, and ensure the protection of the Australia’s national security interests. Building on these arrangements, it is important that improvements to the security practices of all vendors are secured. The effect should be to improve cyber security standards across all suppliers and, in doing so, help to level the playing-field between suppliers.

    - Engage industry to understand Telecoms supply chain risks and the arrangements adopted by operators to mitigate them, and gain regular updates on operators’ major supplier arrangements and TSSR compliance plans.

    - Encourage providers to participate in threat intelligence-led penetration testing scheme and, subject to third party contract arrangements, test operators’ vendor specific arrangements, and share thematic findings across the sector to support a culture of continuous improvement; and increase analysis and reporting on network security and resilience.

- Require operators to work closely with vendors, supported by Government, to ensure effective assurance testing for equipment, systems and software and support specific evaluation arrangements. The new approaches should increase understanding of areas, including engineering and design processes, ongoing product support and vulnerability remediation. The assessment and evaluation of products from different vendors should be the same, as their supply chain has the same level of risk.

- Develop a targeted diversification strategy in order to reduce the over-dependence from 1-2 vendors, and ensure there is a more competitive, sustainable and diverse supply chain. This is critical to drive higher quality, innovation and reduce the risk of national dependency on individual suppliers, regardless of where their HQ is located.

- The new strategy should incentivise entry and growth, including market design and R&D support, cybersecurity evaluation and innovation centres; promoting interoperability and demand stimulation; and attracting established players to Australian market.

- The Government should support market expansion in 5G – including improving access to spectrum, removing barriers to roll-out and promoting new infrastructure models, looking at the development of a more diverse supplier base over time.

- The Government should ensure that any public investment and support is targeted at those areas which can address market failures and yield the strongest security and prosperity benefits to Australia, such as: software-based innovation in core network functions, open architectures in all network domains, and cyber security in small cell technologies.

86. The Government should invest on 5G Testbeds and Trials Programme, in partnership with the industry, looking at end-to-end cybersecurity assurance and compliance to law, standards and regulations; new architecture models allowing operators to use different vendors for difference components; tools for risk mitigation and transparency, and greater interoperability and more open interfaces.

    - The Government should also explore the need for a new national telecommunications lab, with the support of industry and academia. The lab should bring together operators, vendors, industry ‘verticals’ (e.g. manufacturing, healthcare and logistics) and universities, to explore new applications and business models for 5G and beyond.

    - Government could have a number of schemes in place to attract large businesses, including attractive tax incentives (e.g. the lowest corporation tax rate in the G7 and R&D tax credits), a stable regulatory regime and access to talent and labour. These opportunities should be further explored, working with international partners, such as, e.g., the EU and UK, where appropriate.

XENOPHON | DAVIS
LITIGATORS • ADVOCATES

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

27 November 2020

Addendum to Huawei Submission

Following the 2018 ban on Huawei participating in the 5G rollout in Australia the company faced unprecedented public abuse, smears and market damage. However, there was never any credible claim that Huawei had acted inappropriately in Australia or against Australia's interests. Ever. In any way. There was *'no smoking gun'* as former Prime Minister, Malcolm Turnbull, put it. The government's approach *"was a hedge against a future threat"*. That future threat seems to be based on little more than the ethnic origin of the company and the potential for 5G providers to be controlled by the Chinese Communist Party.

As blunt as that risk analysis may be, the security risk does not appear to be mitigated in any way by the the elevation of nominally European 5G providers with manufacturing bases in China.

Huawei is not and never has been a state-owned enterprise. They are in fact an outstanding capitalist success story. They are proudly Chinese but are independent of its state agencies and government manufacturing entities. Ironically, the same cannot be said for Nokia and Ericsson.

It should be a question of great importance to the Committee to establish whether the concerns previously expressed about Huawei are in any way resolved by the purchase of Nokia and Ericsson equipment.

On 25 July 2020 we wrote an article entitled '*Telstra's Ties to Chinese Communist Party Expose Government's Huawei Hypocrisy'.* We attach that document marked as Attachment "A". The article drew attention to the fact that with Huawei excluded all 5G contracts in

XENOPHON | DAVIS
LITIGATORS • ADVOCATES

Australia would likely be met by European providers Nokia and Ericsson. We researched all public sources to show how deeply embedded Nokia and Ericsson's manufacturing base was in China. Despite the public attack upon Huawei, Australia will still be getting Chinese 5G equipment albeit with a European badge. For the benefit of the Committee we expand upon the sources we used for that article and include some relevant updates. All of the links in the footnotes are active as of today's date.

KEY FACTS: NOKIA SHANGHAI BELL

1. Nokia, despite its European headquarters, has extensive manufacturing operations in China through a complex series of partnerships. Nokia Corporation ("Nokia") and China Huaxin Post & Telecommunication Economy Development Center ("China Huaxin") signed an agreement to integrate their China businesses on 18 May 2017 into a new joint venture branded Nokia Shanghai Bell (NSB). Nokia owns 50 per cent of NSB plus a symbolic one share, with China Huaxin owning the remainder. [1]

2. In a Stock Exchange Release on 18 May 2017, Nokia announced "the joint venture will become Nokia's exclusive platform in China for the continued development of new technologies in areas like IP routing, optical, fixed and next-generation 5G; and with the support of Nokia, NSB will continue to look for opportunities in select overseas markets".

3. Nokia Shanghai Bell's board consists of four directors from China Huaxin and four directors from Nokia, with its Chairman Yuan Xin also serving as Party Secretary of the company's Communist Party Branch, as reported in the Sydney Morning Herald.[2]

4. China Huaxin is a subsidiary of China Poly Group, a large-scale central state enterprise under the supervision and management of the State-owned Assets Supervision and Administration Commission of the State Council (SASAC).[3]

[1] https://www.nokia.com/about-us/news/releases/2017/05/18/nokia-and-china-huaxin-sign-definitive-agreements-for-creation-of-new-nokia-shanghai-bell-joint-venture/
[2] https://www.smh.com.au/business/companies/top-5g-suppliers-linked-to-china-s-communist-party-20180812-p4zwzt.html
[3] https://www.poly.com.cn/english/1659.html

XENOPHON | DAVIS
LITIGATORS • ADVOCATES

5. SASAC is "directly subordinated to the State Council". "The Party Committee of SASAC performs the responsibilities mandated by the Central Committee of the Chinese Communist Party," it says on its website.[4]

6. At a signing ceremony of the formation of Nokia Shanghai Bell in 2017, Nokia's former CEO Rajeev Suri proclaimed: "Today's agreement is historic for Nokia and for China, marking the next step of our decades-long commitment to the country and underscoring China's leading role in developing next-generation communication technologies. Nokia Shanghai Bell will enhance our ability to innovate, helping us strengthen ties with communication service providers and expand to new, fast-growing sectors in need of high-performing networks."[5]

7. The joint venture was further strengthened in March 2019 when SASAC hosted the entire Nokia board and Rajeev Suri at a gathering in Beijing. "At the meeting, they exchanged ideas on the state-assets and SOE [State Owned Enterprise] reform, development of communication technology, and cooperation among enterprises," said a news release issued by SASAC.[6]

8. On 27 July 2018, SASAC's then Chairman Xiao Yaqing (pictured below) inspected the Shanghai Nokia Bell headquarters where he "stressed that NSB should" be guided by Chinese leader Xi Jinping's "socialist ideology with Chinese characteristics in the new era and the spirit" of the 19th National Congress of the People's Republic and deepen cooperation with Nokia "to continuously improve the international competitiveness" of the joint venture.

[4] http://en.sasac.gov.cn/2018/07/17/c_7.htm
[5] https://www.nokia.com/about-us/news/releases/2017/05/18/nokia-and-china-huaxin-sign-definitive-agreements-for-creation-of-new-nokia-shanghai-bell-joint-venture/
[6] http://en.sasac.gov.cn/2019/03/29/c_1144.htm

XENOPHON | DAVIS
LITIGATORS • ADVOCATES

9. Huawei is not a member of SASAC nor is it controlled by its directives. Huawei directly controls and owns its manufacturing chain.

10. On 20 February 2020, Nokia's Chief Technology Officer, Oceania, Adam Bryant appeared before a Federal Parliamentary Inquiry into 5G in Australia[7] where he responded to questions from Inquiry member Patrick Gorman MP. Mr Bryant confirmed that Nokia manufactured equipment in China and had a joint venture there. He took on notice a direct question relating to Chinese-manufactured equipment sold by Nokia in Australia.

11. In its response to the question taken on notice regarding whether it sold Chinese-manufactured equipment in Australia Nokia said: *"Nokia has a global manufacturing supply chain and leverages that as appropriate to each customer and market condition."*[8]

KEY FACTS: NANJING ERICSSON PANDA COMMUNICATIONS

12. Ericsson also has complicated manufacturing arrangements in China which, ironically, deeply enmesh it with Chinese state enterprises. Nanjing Ericsson Panda

[7] https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommrep%2Fcf91999e-f860-4639-8a12-653d69062c62%2F0001;query=Id%3A%22committees%2Fcommrep%2Fcf91999e-f860-4639-8a12-653d69062c62%2F0000%22

[8] https://www.aph.gov.au/Parliamentary_Business/Committees/House/Communications/5G/Additional_Documents

Communications Co. Ltd. ("Ericsson Panda") was established in 1992 and is a joint venture between Ericsson, Nanjing Panda Electronics and China Potevio (a company controlled by the State-owned Assets Supervision and Administration Commission of the State Council).

13. Nanjing Panda Electronics ("Panda") on page 37 of its 2019 Annual Report notes Ericsson Panda is 51 per cent owned by Ericsson, 27 per cent by Panda, 20 per cent by China Potevio and 2 per cent by Yung Shing Enterprise Hong Kong.[9]

14. Panda on page 37 of its 2019 Annual Report notes: *"As the biggest production and supply center of Ericsson in the world, ENC is now mainly in charge of the industrialization and mass production of the products that Ericsson Company Limited developed and provides delivery and shipment to customers worldwide."* [10]

15. Ericsson Panda's facility in Nanjing is Ericsson's largest production facility in the world and one of its most important research bases. At the launch of the expanded facility in 2012, Ericsson China's Chairman Mats Olsson (pictured below) declared: *"ENC will play an even more important role in the development of the ICT industry in China and around the world."*[11]

16. Panda on its website notes that it is 29.7 per cent owned by entities controlled by the SASAC, including the defence contractor CEIEC.[12]

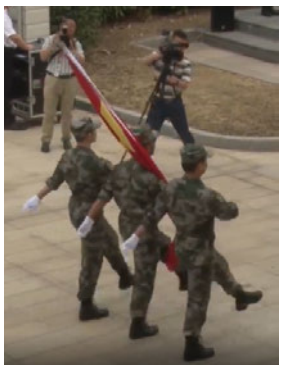
17. On 29 September 2019, Panda issued a media release on how it hosted a series of events to *"celebrate the 70th anniversary of the founding of the People's Republic of China"* and *"arouse the patriotism"* of its employees. The media release said on 26

[9] https://www.panda.cn/uploadfiles/2020/04/20200428090512512.pdf
[10] https://www.panda.cn/uploadfiles/2020/04/20200428090512512.pdf
[11] https://www.ericsson.com/en/press-releases/2012/9/ericsson-inaugurates-new-rd-facilities-in-nanjing
[12] https://www.panda.cn/gqjg/index_393.aspx

XENOPHON | DAVIS
LITIGATORS • ADVOCATES

September 2019, Panda hosted: *"Song of the Motherland - Panda Electronics Celebrating the 70th Anniversary of the founding of New China Literature and Art Festival"*. The media release said: *"The cadres and workers of Panda Electronic gathered together, singing the songs to the motherland."*[13] (pictured below)

18. A video of the flag raising ceremony, featuring military personal and Panda employees holding Chinese flags, was also posted on the Panda website.[14]

19. On 24 June 2020, Panda was named by the US Pentagon[15] as being among 20 *"entities owned by, controlled by, or affiliated with China's government, military, or defense industry". "We envision this list will be a useful tool for the US government, companies, investors, academic institutions, and like-minded partners to conduct due diligence with regard to partnerships with these entities, particularly as the list grows,"* said Pentagon spokesman Jonathan Hoffman.

20. After the Pentagon named Panda on its list, Ericsson issued a statement: *"Ericsson does not source any products from Panda Electronics Group to be used in equipment*

[13] https://www.panda.cn/qyxw/info_395.aspx?itemid=1709&lcid=0
[14] https://www.panda.cn/jcsp/info_33.aspx?itemid=1735
[15] https://nypost.com/2020/06/25/pentagon-releases-list-of-companies-linked-to-chinese-military/

utilized in any of Ericsson's products." [16] Ericsson, however, did not say whether it sourced products from the Ericsson Panda facility in Nanjing.

21. Ericsson China Chairman Mats Olsson in 2012 referred to the Ericsson Panda facility as a "*global production and supply unit*".[17]

22. On 19 February 2020, Ericsson's Australia and New Zealand Head of Government and Industry Relations Michelle Phillips appeared before a Federal Parliamentary Inquiry into 5G in Australia[18] hearing, where she responded to questions by Inquiry Deputy Chair Hon Ed Husic MP regarding Ericsson's operations in China. Ms Phillips confirmed: *"Ericsson does have manufacturing facilities and capabilities in China".* Ms Phillips had to take several questions on notice.[19]

23. On 5 March 2020, Ms Phillips provided a written response to the questions taken on notice on the day of the hearing. [20] In response to a question on whether Ericsson manufactures products in China, Ms Phillips said: *"Ericsson is proactively increasing the flexibility in its supply chain, sourcing and product development to move production closer to our customers to ensure we can respond quickly to their needs. We have a flexible global supply chain with production facilities in the United States, Brazil, China, Estonia, Hungary, India, Malaysia, Mexico, Poland, and Romania."* It is of considerable concern that such an oblique answer can be given to a question that is, presumably, of considerable importance to the Committee.

24. In her written response to the Federal Parliamentary Inquiry into 5G in Australia, Ms Phillips further confirmed: *"Some products that Ericsson supplies to customers in Australia are manufactured in China."*

25. We note that Ericsson is supplying equipment for Telstra[21] and Optus's[22] 5G networks in Australia.

---

[16] https://www.reuters.com/article/us-ericsson-panda-idUSKBN2481Q3
[17] https://www.ericsson.com/en/press-releases/2012/9/ericsson-inaugurates-new-rd-facilities-in-nanjing
[18] https://www.aph.gov.au/Parliamentary_Business/Committees/House/Communications/5G
[19] https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommrep%2Fac13b55a-614a-4f09-bfd0-38a2c53f492e%2F0001;query=Id%3A%22committees%2Fcommrep%2Fac13b55a-614a-4f09-bfd0-38a2c53f492e%2F0000%22
[20] https://www.aph.gov.au/Parliamentary_Business/Committees/House/Communications/5G/Additional_Documents
[21] https://www.ericsson.com/en/news/2019/7/ericsson-and-telstra-complete-australias-first-5g-end-to-end-standalone-call
[22] https://www.ericsson.com/en/news/2019/11/optus-partners-with-ericsson-for-5g

XENOPHON | DAVIS
LITIGATORS • ADVOCATES

26. We urge that a set of security criteria be applied to all equipment suppliers that is 'colour blind' to the ethnicity of its executives or the location of its headquarters and focuses on a definable threat that can be objectively and properly assessed.

Xenophon Davis

Attachment "A"

News

Telstra's Ties To Chinese Communist Party Expose Government's Huawei Hypocrisy

Written by Scott Rochfort

On July 25, 2020

Last month it was revealed the co owner of Ericsson's main Chinese production and research facility, which supplies 5G equipment to Australian customers including Telstra, was on a US Defence Department list of companies with supposed links to the People's Liberation Army.

A statement from the Pentagon claimed Ericsson's joint venture partner, the Chinese State majority owned
Panda Electronics, was a "Communist Chinese

Latest Post


Mark Davis: David McBride's prosecution is not in the public interest


Xenophon Davis launches legal action against financial industry 'ombudsman'


Julian Hill: The political persecution of Julian Assange is unconscionable


Afghan Files Whistleblower Launches Unprecedented Challenge Against Prosecution

Witness J: "I take no enjoyment in being Australia's first secret

military" company. Oddly that news didn't trigger much interest from the security hawks in Australia regularly quoted in the media.

All that blonde hair may have overwhelmed Australia's intelligence analysts as it is now apparent Ericsson and Nokia are both deeply enmeshed in corporate and production partnerships with the Chinese Communist Party.

Ironically, our client Huawei, which has been barred from supplying 5G equipment in Australia, is an independent and privately owned capitalist enterprise.

Nokia escaped attention from last month's salvo from the Pentagon but an analysis of its manufacturing and research facilities in China reveals the depth of its links there. Nokia's main Chinese business, Nokia Shanghai Bell, is half owned by the Chinese State and substantially under its control.

The joint venture, which manufactures telecommunications equipment is an "integral part" of Nokia's global research and development into a "vast array" of technologies including wireless access, Cloud RAN and 5G.

Given the hysteria over Huawei, it is extraordinary that Ericsson and Nokia's CCP links have been totally ignored in Australia. For researchers (hint, the media) we attach as many hyperlinks below as possible. See for yourself.

Nokia Shanghai Bell follows Beijing's tune

One clear sign that Nokia Shanghai Bell

has stronger ties with Beijing than Helsinki, was when the facility was inspected by the chairman of the State owned Assets Supervision and Administration Commission of the State Council (SASAC), which co owns the facility with Nokia. SASAC is the main holding company for Chinese state owned enterprises.

During the visit in 2018, SASAC chairman Xiao Yaqing issued some very clear directives to Nokia Shanghai Bell staff.

Wearing a yellow lab coat, Xiao stressed Nokia Shanghai Bell should be guided by China's Communist Leader Xi Jinping's "socialist ideology with Chinese characteristics in the new era and the spirit" of the 19th National Congress of the People's Republic. He said Nokia Shanghai Bell should make a "thorough study of the important discourse of reform and development of state owned enterprises and [the] Party's construction said by Xi Jinping".

With SASAC deputy chairman Peng Huagang smiling behind him, Xiao had an "in depth exchange" with one of the researchers at the R&D facility and gained a further understanding of the ground breaking technologies it was developing.

It is understandable Xiao issued this order given SASAC's key role is to perform "the responsibilities mandated by the Central Committee of the Chinese Communist Party". And it is likely these statements resonated with Yuan Xin, the Party Secretary of the Nokia Communist Party Branch who also happens to be the chairman of Nokia Shanghai Bell.

SASAC had approved the formation of the Nokia Shanghai Bell joint venture between its subsidiary Huaxin and the Finnish technology firm Nokia the year before Xiao's inspection tour.

According to Huaxin, Nokia Shanghai Bell is under the "supervision" of the SASAC and is described as a "strong national asset" in China.

A blossoming comradeship in China

At the signing ceremony marking the formation of Nokia Shanghai Bell in 2017, Nokia's former CEO

Rajeev Suri proclaimed: "Today's agreement is historic for Nokia and for China, marking the next step of our decades long commitment to the country and underscoring China's leading role in developing next generation communication technologies. Nokia Shanghai Bell will enhance our ability to innovate, helping us strengthen ties with communication service providers and expand to new, fast growing sectors in need of high performing networks."

The joint venture was further strengthened in March 2019 when SASAC hosted the entire Nokia board and Rajeev Suri at a gathering in Beijing.

> "At the meeting, they exchanged ideas on the state assets and SOE [State Owned Enterprise] reform, development of communication technology, and cooperation among enterprises," said a news release issued by SASAC.

Nokia gets excellent reception in Canberra

Strangely, Nokia's management team in Australia appear to have missed the memo from their Finnish headquarters on Nokia's blossoming relationship with the Chinese Communist Party's flagship investment vehicle.

Nokia Chief Technology Officer Oceania, Adam Bryant had some difficulty answering some questions related to Nokia's operations in China when he fronted a Federal parliamentary committee in February into the "deployment, adoption and application of 5G in Australia".

When asked by committee member MP Patrick Gorman if Nokia had to set up a joint venture for manufacturing in China, Bryant answered: "Yes, there is a requirement for a joint venture."

Gorman then asked: "What were the requirements in terms of protection or handing over of intellectual property?"

Bryant had to take the question on notice.

The questioning continued.

Mr Gorman: *"What were the requirements in terms of protection or handing over of intellectual property?*

Mr Bryant: I'll take that on notice.

Mr Gorman: *You'll probably also want to take this on notice. Were there any other administrative or regulatory conditions of manufacture that would be different in Nokia's normal business practices?*

Mr Bryant: I apologise; I'll have to take that on notice.

Mr Gorman: *I expected you would, but I just needed to ask. We asked one of your competitors similar questions yesterday, and I think it's only appropriate that we make sure that those questions are asked of each and we don't single one out.*

Mr Bryant: Thank you.

The competitor the Labor MP was referring to was Ericsson.

The above transcript appears to be the only interrogation by Australian politicians (if it can be called that) that Ericsson and Nokia have faced in relation to their supply of 5G equipment to Australia from facilities it co owns with the Chinese State.

Following the ban on Huawei from Australia's 5G network by the Turnbull government in 2018, Nokia and Ericsson are the only major suppliers left to supply equipment to the next generation mobile network.

Not once in the hearings was there
any mention of Nokia or Ericsson's joint ventures in China being co owned by the Chinese state.

That was it. Wet lettuce interrogation over.

The parliamentary committee handed down its report in March, with not a single mention of Nokia and Ericsson's joint ventures in China. Nor their strengthening relationships with the Chinese State.

Huawei has been endlessly vilified by Australian politicians in the most extreme terms for little more than being Chinese. How stark is the contrast when they are dealing with Scandinavian providers whose equipment is made under the ownership and direction of the Chinese Communist Party.
Ironically, Huawei's equipment is not.

← Previous Post Next Post →

The Hon Malcolm Turnbull MP

MINISTER FOR COMMUNICATIONS

11 AUG 2015

Mr Xichu (James) Zhao
CEO, Huawei Australia
Level 6, Tower B, 799 Pacific Highway
Chatswood NSW 2067

Huawei and the Telecommunications Sector Security Reforms

Dear Mr Zhao

Thank you for your letter dated 31 July 2015 concerning the proposed Telecommunications Sector Security Reforms (TSSR). I appreciate your organisation's ongoing commitment to improving cyber security in Australia and I understand your concerns about the recent media article.

TSSR is part of the Australian Government's efforts to ensure that national security issues within the telecommunications industry can be handled appropriately and proportionately. The proposed TSSR framework aims to improve the security of Australian carriers and carriage service providers. It does this by taking a risk management approach to the security of Australian telecommunications networks.

Under the proposed framework, telecommunications companies would be free to consider any commercial options for equipment and services. Australia's security agencies will assist companies by providing advice and guidance on security risks.

I can assure you that the obligations under TSSR do not apply to suppliers and do not seek to exclude any specific supplier from offering services or equipment to the Australian telecommunications market. It is regrettable that recent media attention has led to questions from current and potential customers regarding your products and services.

I trust this information has been of assistance in clarifying the intent of the proposed TSSR framework.

Yours sincerely

[redacted]

Malcolm Turnbull

CC
Senator the Hon George Brandis QC, Attorney-General.

Parliament House, Canberra ACT 2600 | Telephone 02 6277 7480
287-289 New South Head Road, Edgecliff NSW 2027 | Telephone 02 9327 3988