Huawei Australia submission to the Department of Home Affairs

Security Legislation Amendment (Critical Infrastructure) Bill 2020

27 November 2020

Introduction

1. Huawei Australia is grateful for the opportunity to make a submission to the Department of Home Affairs for the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

2. Huawei Australia is a privately owned Australian based company and it is our foremost duty and obligation to comply with Australian laws including those in the Security Legislation Amendment (Critical Infrastructure) Bill 2020. The parent company of Huawei Australia is free of state ownership and is fully owned by our staff.

3. Huawei has and always will build its technology with Cyber Security Safety as a central commitment to our customers. We understand the security requirements from Governments around the world, and we build our products to meet their needs.

4. We build our technology assuming someone, somewhere will want to do bad things to our products - organized crime, terrorists, state actors, local hackers etc. It's why Huawei puts in place world leading cyber security protocols and systems.

5. We are so confident of our credentials in this area we are the only vendor that has opened itself up to totally independent evaluation and testing. This is something we have continually offered to the Australian Government, and still do.

6. 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.

7. Despite our proven track record of Cyber Security our telecom network equipment business in Australia has been significantly impacted since the introduction of the Telecommunications Sector Security Reforms (TSSR) legislation in 2018 with nearly 1,000 job losses and over $100 million lost in ICT research and development funding here in Australia.

8. The TSSR legislation was intended to deliver more secure telecom networks for Australians – a mission which we support – however it seems that Huawei has been the collateral casualty of TSSR legislation that has not been properly thought through with regard to its own implications. Moreover, the TSSR has not achieved its original intention of delivering more secure networks.

9. This is because rather than addressing the security merits of vendors on a non-discriminatory basis they are assessed on the basis of their country of origin – which in our case as a Chinese company has seen us suffer severe negative consequences.

10. 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. The lack of due and transparent process is deeply concerning.

11. Given that 5G equipment from Nokia and Ericsson [see addendum] continues to be made in China – in partnership with companies state-owned by the Chinese Government – and is then deployed on 5G networks without any testing then it hard to see how this delivers a more secure outcome.

12. We fully accept and support that Australia has a need to protect its critical infrastructure but we do not think it advisable to follow the same path as has been followed in the TSSR legislation with vendors banned simply on the basis of their country of origin.

13. Huawei currently supplies our equipment to be used in critical infrastructure including rail networks, emergency services radio systems and solar power networks and has a spotless security record in these areas.

14. However, if a similar approach is taken in this legislation as was taken in the TSSR legislation – that is not facts and evidence based then our faultless record will be ignored and we will suffer negative consequences in these areas too.

15. Our recommendation is that the Department of Home Affairs take a more deliberative approach to protecting critical infrastructure and rather than simply banning vendors for their country of origin actually properly assesses risk based on a full testing process of vendor equipment on an ongoing basis.

Executive Summary

16. Huawei Australia understands, fully accepts and supports the need for the Department of Home Affairs to secure Australia's critical infrastructure from external threats and stands ready to support such an initiative in any way in which we can do so.

17. Huawei Australia has operated safely and securely in Australia for sixteen years here in Australia and has always meticulously obeyed all local laws and regulations.

18. To be absolutely clear 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.

19. Clifford Chance 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. In any event, our foremost obligation has always been to comply with Australian laws and regulations.

20. 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, organization 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.

21. As well as our long standing involvement in building out mobile and fixed-line telecom networks here in Australia Huawei has also built up an Enterprise business over the last sixteen years in Australia in which we have delivered our equipment to critical infrastructure projects.

22. We have worked with Sydney Trains for many years on delivering the GSM-R based radio systems that help provide radio communications on the Sydney Trains network – we have delivered safe and secure technology over this period with no security incidents.

23. In addition, Huawei has also supplied our radio technology to NSW Ambulance to help deliver their radio network services that deliver their essential communications – this has also been delivered in a safe and secure manner.

24. Huawei was also successful in winning the contract to deliver the radio access system using GSM-R technology to the Perth Metro project being delivered by the West Australian Government – although we are no longer involved in this project.

25. Huawei also supplies our inverter technology to solar networks being rolled out across the country by solar network installation companies. Huawei Australia does not own or operate these solar networks – we simply supply our inverter technology.

26. Huawei's involvement in these critical infrastructure projects such as Sydney Trains or with others is sometimes conducted directly with the customer but can also be delivered via a third-party contractor.

27. Having now been excluded from the 5G market by the introduction of the TSSR the vast majority of Huawei Australia's current and future revenue streams come from the Enterprise segment.

28. Huawei Australia wants to continue being able to deliver services to our customers in the Enterprise sector and wants the Security Legislation Amendment (Critical Infrastructure) Bill 2020 to allow us to do this.

29. We fear that a similar approach as taken in the TSSR legislation – without due process and transparency - will not enable us to do this and would cause additional significant harm to our company.

30. As things stand under the TSSR as a Chinese company Huawei is banned from delivering 5G technology, yet Nokia and Ericsson continue to manufacture their 5G hardware in China – in partnership with state-owned companies – and import it into Australia onto 4G and 5G networks without testing.

31. In fact the TSSR legislation permits Telstra and Optus to install 5G equipment made in China by the Ericsson/Panda Electronics joint venture. 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. Ericsson has defended this relationship by saying that Panda Electronics is only a 'minority shareholder' in the venture - as if that makes a difference.

32. Either the Australian Government did not know the alternative suppliers to Huawei both manufactured 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.

33. Taking these facts into consideration the TSSR has not only increased 5G costs for Australian network operators and consumers but has actually failed to deliver 5G networks that are any more secure given that equipment is not being tested or evaluated – it is therefore vitally important that a different approach is taken with regard to critical infrastructure.

34. We recommend that the Department of Home Affairs take a different approach to protecting critical infrastructure and adopts a 'Zero Trust' approach towards allowing vendors to participate as the best way to protect Australia's critical infrastructure.

35. All vendors should be subject to an independent review and testing of their equipment on an ongoing basis no matter their country of origin to ensure compliance with the most stringent security requirements.

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. For example, the global 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.

Our recommendations

37. The best way to assure reliable critical infrastructure is to have a comprehensive approach to risk and resilience, which includes verifiable conformance and testing protocols. When it comes to managing risks in cyberspace, the best approach is to distrust everyone and put them through the most rigorous and objective scrutiny.

38. Making a determination that a supplier is trustworthy based on the country in which it is headquartered is a misguided and dangerous approach.

39. 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.

40. We recommend a cybersecurity approach to critical infrastructure that includes two design principles and three pillars. The two principles are trust minimization and the assumption of breach.

41. Trust Minimization; Trust should be considered a fatal design flaw. Therefore, any security solution designed for critical infrastructure should minimize, as much as possible, the degree of trust in the underlying components, services, and personnel. Trust should be proven based on facts and should not be assumed.

42. Assume Breach: This is a concept that was coined in the early 2000’s by Kirk Bailey, who suggested that organizations should build their networks based on the assumption that a well-funded adversary would be able to infiltrate any system.

43. These principles complement each other and should be the foundation for a robust risk-mitigation framework. Trust-minimization and assume-breach have successfully proven themselves under extreme, hostile conditions for the past decade. This rigorous and evidence based approach should be adopted rather than a dangerously superficial view on the ethnicity of the vendors involved.

44. Of the three core pillars of cyber security the most obvious is that of standardisation that provides a common set of guidelines, requirements, and recommendations in a transparent, verifiable, and reproducible manner.

45. Standardization provides experts and laymen, businesses, regulators, and customers with a clear and common understanding of good versus bad. Once set, these common guidelines, requirements, and recommendations are continuously validated and verified by operators and regulators in the domain or industry covered.

46. The second pillar is built around aligning verification and testing with the principle of trust minimization – forming an essential part of a holistic, risk-mitigation strategy.

47. Verification ensures that products and services provided by any vendor in critical infrastructure satisfy a set of well-defined requirements, thereby reducing the risk that a product behaviour is inconsistent with the agreed specification, including in failure scenarios.

48. Security testing goes a step further by ensuring that the system security properties are not violated even under hostile and/or unpredictable conditions. Various security certification schemes have developed over the past thirty years for the evaluation of vendors' and operators' security posture.

49. For example, in the global mobile technology sector these include product-specific standards efforts such as ISO 15408 (Common Criteria) and GSMA/3GPP NESAS/SCAS, as well as company-level risk management schema such as ISO/IEC 270xx, ISO/IEC 28000, and ISO 22301, to name a few.

50. The third and final pillar relates to delivering multi-level cyber resiliency which ensures that systems will be able to perform their most critical tasks even when under attack.

51. The concept of cyber resiliency is a flexible one that can be adapted to various scenarios. Every organization has different goals and priorities, so each organization has to determine what its mission-critical tasks are for the critical infrastructure in question.

52. As we have already submitted one of the core weaknesses of the TSSR legislation is the way in which it discriminates against vendors based on their country of origin rather than actually addressing the key and underlying cyber security issues.

53. Excluding certain vendors while trusting others without assessing and addressing real cybersecurity risk, makes no sense from an economic or cybersecurity perspective.

54. Trustworthiness does not play a role in cybersecurity. What matters far more is the transparency of telecom suppliers' operations, including whether and how they provide ongoing support to the operator after equipment is installed.

55. Selecting a supplier should be based on the quality and reliability of its products, their demonstrable conformance to standards and best practices, as well as compliance with regulatory and contractual requirements.

56. Banning vendors reduces competition and ironically increases the cybersecurity risk; the UK's Intelligence and Security Committee (ISC) stated in July 2019 that, "limiting the field to just

two vendors,.., would increase over-dependence and reduce competition, resulting in less resilience and lower security standards.”

57. Looking at mobile telecommunications infrastructure, currently, the TSSR (power of direction) makes the entire ICT infrastructure less secure by increasing the over-dependence from just two vendors.

58. Rather than reduce choice in this manner – which leads to less competition and increased costs - 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.

59. As we have argued previously the glaring weakness of the TSSR legislation is that it doesn’t make Australia’s telecommunications networks any more protected from cyber security threats because it doesn’t address the key underlying issues – preferring to simply ban vendors based on their country of origin.

60. Huawei doesn’t want the same mistake to be made in the critical infrastructure space and would recommend that the Department of Home Affairs construct a proper end-to-end testing regime for all vendors regardless of their country of origin in order to deliver an end-to-end solution.

61. There is a valid argument to be made for voluntary testing of hardware in the consumer space as the Department of Home Affairs has initiated as part of its regulatory approach towards connected devices in the Internet of Things.

62. A voluntary approach for vendors in the consumer space is defensible as consumers can then make their own choices based on what steps have been taken by the vendor to deliver a secure product.

63. However, for mobile networks and critical infrastructure we recommend that there should be a mandatory testing platform in place for all vendors – no matter their country of origin – in order to deliver the most robust cyber security framework.

64. Huawei believes Australia should implement a policy that enables independent testing and verification of ALL vendors’ technology. Huawei has nothing to hide, but we have documented evidence that our competitors in the mobile technology space do not support open, transparent and independent testing of their equipment in Australia and have directed the telecommunications industry not to support such an important initiative.

65. 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.

66. The reality is that Australia will lose out in the long-run by not adopting a proper evidence-based approach to cyber security given the fact that so much new technology will emerge from Asia in the coming years – with a significant portion of that coming from China itself.

67. A policy of simply refusing technology on the basis of the country of origin of the vendor will have very large economic consequences while the rest of Asia and the world will get the full benefits of having access to world’s best telecommunications and IT products.

68. Finally, we formally and respectfully request an opportunity to present to you in relation to this submission so that we may elaborate on the same and be subject to your questions.