paloalto® NETWORKS

26 November 2020

Parliamentary Joint Committee on Intelligence and Security
Committee Secretariat
PO Box 6021
Australian Parliament House
Canberra, ACT, 2600

RE: Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms (TSSR)

Palo Alto Networks appreciates the opportunity to provide comments to the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) inquiry into *Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms*. We are pleased to see the Australian Parliament taking interest in telecommunication security and reviewing the measures the Government should take to manage the national security risks of espionage, sabotage and foreign interference issues in Australia's telecommunication networks.

Palo Alto Networks is the largest cyber security company in the world. Palo Alto Networks secures the networks and information of more than 77,000 enterprise and government customers in 150+ countries to protect billions of people globally, including in Australia. 95% of the Fortune 100 and more than 71% of the Global 2000 rely on us to improve their cyber security posture. We work with an array of organisations across all verticals, including Internet Service Providers (ISPs) and Telecommunication Providers (Telcos). We have conducted numerous "proof of value" tests around the world where we have worked with mobile network operators and ISPs to deliver capabilities that find and block malware and other cyberattacks within mobile tunnels.

In undertaking this review, we would encourage the PJCIS to consider any related impacts or overlap with the Department of Home Affairs' call for views on the *Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020,* which also addresses security measures for the telecommunications sector. We encourage the Australian Government and Parliament to ensure reporting and obligations under these two acts are aligned.

Australia Faces Increasing Cyber Threats

Globally, countless adversaries are willing to steal information, illegally make profits, and undermine their targets. Over the last decade the level of sophistication employed by

adversaries (in particular, cybercriminals) has dramatically increased. While some criminals continue to compromise networks using publicly known vulnerabilities that have known mitigations, others are leveraging sophisticated attack tools to help find new exploits and automate and scale their attacks. Today, cybercriminals operate like a sophisticated business – they employ people, they have hierarchies and processes, and unfortunately they are making a sizeable profit from their clandestine activities.

Palo Alto Networks threat intelligence team, Unit 42, confirms this trend. In an annual 2019 report on one Nigerian cybercriminal organisation, assigned the name "SilverTerrier", Unit 42 detailed their rapid expansion from just a few individuals experimenting with malware purchased online, to an organisation encompassing around 480 different actors and groups collectively producing more than 81,300 samples of malware linked to 2.1 million attacks worldwide.[1] The report also detailed that the frequency of SilverTerrier's attacks had dramatically increased. In 2018, there were an average of 34,039 attacks per month against Palo Alto Networks customer base. In 2019, this number climbed to an average of 92,739 per month – peaking at 245,637 attacks in the month of June 2019. While our customer base was protected against these attacks, the statistics demonstrated the widespread proliferation of cybercriminal activities.

An increase in cyber crime has been experienced across Australia. In 2018, close to one in three Australians were victims of cyber-crime.[2] The Australian Cyber Security Centre (ACSC) receives a report of cyber-crime every ten minutes.[3] These attacks come at a significant cost to the Australian economy and our society. They also breed a lack of confidence and faith in online applications and can slow digital transformation. It is estimated that cyber incidents targeting small, medium and large Australian businesses costs the economy up to $29 billion per year, or 1.9% of Australia's gross domestic product.[4]

High profile incidents of cyber crime have exemplified the speed with which cyberthreats can propagate globally, how rapidly adversaries can adapt to security responses, and how easily a compromise can impact an organisation's core functions or services. In 2020, there has been increased reporting of cyber incidents affecting big Australian companies; a large Melbourne-based global logistics company has been hit twice by ransomware attacks, cyber incidents have also affected a government agency, resource company and a financial services company. On 19 June, Prime Minister Scott Morrison announced that Australian organisations, across a range of sectors and levels, were being targeted by a sophisticated state-based cyber actor. This is a trend that is likely to continue, as the ACSC notes in their *2019-20 Annual Cyber*

[1] https://unit42.paloaltonetworks.com/silverterrier-2019-update/
[2] https://www.staysmartonline.gov.au/news/reverse-threat-cybercrime/stay-smart-online-week-2019
[3] https://www.zdnet.com/article/australians-are-reporting-cybercrime-activities-once-every-10-minutes/
[4] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Threat Report.[5]

Address Cyber Threats At Scale Via A "Clean Pipes" Policy

Palo Alto Networks believes that to stop the economic loss associated with cyber crime and the impacts of a widespread cyberattack, Australia should harden its national defences and address these threats at scale via leveraging ISPs to detect and stop cyberattacks in real time. This approach recognises that the vast majority of cyberattacks that occur in Australia leverage Australian ISP or telco infrastructure. In particular, Palo Alto Networks supports the adoption of a national clean pipes policy and encourages the Government to work with Industry and play an active role in driving its adoption. The Australian Government and the Australian Strategic Policy Institute (ASPI) both have talked about the merits of clean pipes, and Telstra has announced a clean pipes strategy (all detailed below).

'Clean pipes' is the idea that ISPs could provide security services to their customers to deliver a level of default security.[6] A key advantage of clean pipes is that it brings advanced scalable protection to an ISP's entire customer base, which is particularly important to the majority of customers who lack the skills and resources to provide for their own security - such as medium and small businesses as well as everyday Australians.[7]

The Australian Government appears to be interested in a clean pipes policy. On 30 June 2020, Prime Minister Scott Morrison announced a funding commitment to 'prevent malicious cyber activity from ever reaching millions of Australians across the country by blocking known malicious websites and computer viruses at speed'.[8] The *2020 Cyber Security Strategy* went further to note the importance of businesses, particularly telecommunications providers, automatically blocking known malicious threats to protect Australians and Australian businesses from cyberattacks at speed and scale. It noted that the Government will, over the life of the Strategy, support businesses to implement threat-blocking technology that can automatically protect citizens and businesses from known malware and trojans.[9] This would help prevent and minimise harm to organisations and Australian citizens who cannot protect themselves.[10]

The Strategy also notes Telstra's "Cleaner Pipes" initiative announced in May 2020. Telstra should be lauded for paving the way with this initiative, which involves Telstra's Domain Name System (DNS) filtering, where millions of malware communications are being blocked as they try to cross Telstra's networks. While there are limitations of DNS filtering as a technical solution to

[5] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020
[6] https://www.aspi.org.au/report/clean-pipes-should-isps-provide-more-secure-internet
[7] https://www.aspi.org.au/report/clean-pipes-should-isps-provide-more-secure-internet
[8] Scott Morrison, 'Nation's largest ever investment in cyber security', media release, 30 June 2020
[9] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
[10] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

delivering what some might consider a more comprehensive clean pipes solution, this announcement is a great step in the right direction.[11]

We recommend that the Government determine how it might broaden and scale a clean pipes approach, as well as provide incentives (economic or otherwise) for ISPs and telcos to take similar actions to help build Australia's collective defences. Specifically, Palo Alto Networks recommends that the Government look at ways to encourage and incentify ISPs and Telcos to maintain constant real-time visibility across traffic passing through their networks and be able to detect and stop in real time cyber security threats within that traffic. Having this capability be available to all ISP and Telco customers would be a great next step. While ISPs and telcos secure their own corporate infrastructure (in line with TSSR obligations), not all provide security to end-customers.

As ASPI notes in its recent paper 'Clean pipes: Should ISPs provide a more secure internet?', while there is 'no legal impediment to ISPs providing some level of protection to their customers (excepting techniques that would be privacy-invading), there is also no incentive to provide these services.'[12] The paper also goes further to note that there is no community expectation that ISPs will deliver this service nor is there any ' legal or regulatory obligation that has pushed ISPs to provide enhanced default security services.'[13] The Government should consider as part of this review how it can incentivise and support ISPs and Telcos to provide these services to the broader community. A clean pipes solution is a key mechanism to protect Australian Governments, businesses and families from cyberthreats, and make Australia a less attractive target to cyber adversaries.

Summary of Recommendations

Palo Alto Networks recommends that the PJCIS:

1. Note the merits of adopting a clean pipes solution to protect Australian Governments, businesses and families from cyberthreats, and make Australia a less attractive target to cyber adversaries, and
2. Look at ways to encourage and incentify ISPs and Telcos to maintain constant real-time visibility across traffic passing through their networks and be able to detect and stop cyber security threats in real time within that traffic for all customers.

Conclusion

We would be happy to discuss our ideas further. For more information, please contact [redacted] head of government affairs and public policy, Australia and New Zealand, at

[11] Please see: https://australiancybersecuritymagazine.com.au/australians-going-online-can-be-secure-by-default/
[12] https://www.aspi.org.au/report/clean-pipes-should-isps-provide-more-secure-internet
[13] https://www.aspi.org.au/report/clean-pipes-should-isps-provide-more-secure-internet

paloalto® NETWORKS

[redacted]

For more information on a comprehensive approach to securing networks and data please visit: https://blog.paloaltonetworks.com/2020/09/securing-5g-networks-and-data/

About Palo Alto Networks

Palo Alto Networks, the global cyber security leader, is shaping the cloud-centric future with technology that is transforming the way people and organisations operate. Our mission is to be the cyber security partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organisations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.

Palo Alto Networks is committed to helping Australian Governments and private organisations across all industry sectors embrace the digital world safely and protect their business operations from cyberattacks. Many of our customers are Australia's largest enterprises and government organisations. We also have undertaken a range of activities that contribute to strengthening Australia's cyber security posture, including hosting roundtables with government and enterprise stakeholders to promote thought leadership; and partnering with the education sector to design cyber security courses. For more information see https://www.paloaltonetworks.com.au/