# Response to the 2023-2030 Cyber Security Strategy Discussion Paper

## About Vocus

Vocus, Australia's specialist fibre and network solutions provider, owns and operates Australia's second-largest intercapital fibre network. In total, the Vocus network comprises 25,000km of secure, high-capacity fibre supported by the 4,600km Australia Singapore Cable (ASC) and the 2,100km North West Cable System (NWCS). Vocus delivered the 4,700km Coral Sea Cable System (CS2) connecting Australia to Papua New Guinea and the Solomon Islands on behalf of the Australian Government, and is currently deploying the Darwin-Jakarta-Singapore Cable system (DJSC) – the first international fibre cable connecting Australia's North to Asia. Vocus is also in the process of acquiring Challenge Networks, a private mobile network operator which has designed and deployed mobile voice and data networks throughout the Indo-Pacific.

## Executive Summary

Vocus welcomes the opportunity to respond to the 2023-2030 Australian Cyber Security Strategy Discussion Paper. As the owner and operator of international fibre-optic cable infrastructure, Vocus' response will focus on the international elements of the paper.

Vocus submits that Australia should take a leadership role in establishing secure digital infrastructure in the Indo-Pacific to enhance the connectivity and capability of Australia and our regional neighbours.

While Australians are fortunate to have virtually universal access to voice and broadband services, many people living throughout the Indo-Pacific still lack access to basic connectivity. The cyber security challenges faced by our regional neighbours are vastly different to Australia's, given the lack of fundamental digital infrastructure required to access online services by Governments, businesses, and citizens alike.

Australia has had some notable successes in establishing digital infrastructure in the Pacific, including the delivery of the Coral Sea Cable System with Papua New Guinea and the Solomon Islands and plans for further submarine cable investments in the region. However, these efforts have, to date, been largely ad-hoc and reactive to immediate issues. Much of the region continues to be connected by ageing, low-bandwidth digital infrastructure, and a lack of commercial investment incentives means the digital divide – particularly in the Pacific Islands – will continue to grow.

In recent years, broader geo-political considerations in the region have made Australia increasingly attractive as a safe haven for international connectivity. International operators seeking to diversify their digital infrastructure to mitigate risks in the region are attracted to Australia's stable political, regulatory, and economic environment – leading to an increase in proposals to connect new submarine cables to Australia. These cables, which carry around 97 per cent of global data traffic, are the backbone of the internet.

As part of its 2023-2030 Cyber Security Strategy, Australia should seek to leverage its emerging position as an Indo-Pacific cable hub by partnering with private-sector operators to extend cable infrastructure to underserved nations throughout the region. Providing this foundational infrastructure is the first step in lifting the cyber security and resilience of the region and would enhance Australia's connections – literally and figuratively – with our regional neighbours.

Australia should also seek to leverage our well-developed datacentre industry to enable our regional neighbours to store and process their data in Australia. This should include establishing a legal framework which maintains the sovereignty of the data and provides the same high standard of security that the Australian Government requires of its own data.

## Response to Discussion Paper Questions

*3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?*

*4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?*

**Secure and sovereign telecommunications infrastructure in the Indo-Pacific**

Vocus welcomes the Government's announcement that it will integrate Australia's domestic and international cyber strategies. We support the Government continuing to work in partnership with our Indo-Pacific neighbours to improve their digital connectivity, which will be fundamental to realising their economic development objectives and building a cyber-resilient region.

Access to digital infrastructure is the foundation of building cyber resilience in the region. As Geoff Huston, Chief Scientist at APNIC (Asia Pacific Network Information Centre, the Internet address registry for the Asia-Pacific region) recently explained, the Pacific has long been a 'transit zone' for digital infrastructure – where the major economies located on the rim of the Pacific Ocean build point-to-point cable systems, bypassing Pacific Islands nations and leaving them dependent on low-capacity satellite services.[1]

It is only in recent years that we have seen submarine cable systems proposed to smaller nations in the Pacific. For example, in 2020 the Australian Government announced it was partnering with Japan and the United States to finance a cable to the Republic of Palau.[2] In 2021, Australia, Japan, and the US agreed to jointly fund a new submarine cable system connecting Federated States of Micronesia, Kiribati, and Nauru.[3] There are opportunities for Australia to invest further in a region still struggling with global connectivity, with many countries in the Indo-Pacific still reliant on a single cable connection, and others relying on expensive satellite connections.

Australia's cyber security strategy should not overlook the physical elements of the internet. Access to, and influence over, submarine cable infrastructure can have direct effects on security. Submarine cables are subject to natural threats and threats caused by intentional and unintentional human activity. Potential threats posed by malicious actors include deliberately cutting cables, tapping them, and cyber-attacks.[4] Multiple parts of the submarine cable supply chain can potentially be compromised, enabling the interception of data, surveillance, and traffic disruption.[5] There are also a range of potential risks to the reliability of cables including damage caused by seismic activity, fishing, and vessel anchors. Countries with only one cable are especially vulnerable to outages, as was seen in Tonga when its sole submarine cable was damaged by a volcanic eruption in 2022, taking almost 6 weeks to repair.

There is a strong desire across the Indo-Pacific for better connectivity and to address the vulnerabilities in existing cable networks. Submarine cable assets are critical in bridging the digital divide in the region as capacity demand increases. In an address to ASPI's Sydney Dialogue in April 2023, Samoa's Prime Minister, Fiame Naomi Mata'fa highlighted that "reliable, fast, affordable international connectivity opens up huge potential for small island states. We have seen this in the Pacific once a cable was landed."[6]

---

[1] The politics of submarine cables in the Pacific, Geoff Huston, APNIC, 2 June 2022, https://blog.apnic.net/2022/06/02/the-politics-of-submarine-cables-in-the-pacific/

[2] Australia is partnering with Japan and the United States to finance Palau undersea cable, AIFFP, 28 October 2020, https://www.aiffp.gov.au/news/australia-partnering-japan-and-united-states-finance-palau-undersea-cable

[3] Joint Statement on Improving East Micronesia Telecommunications Connectivity, U.S. Department of State, 11 December 2021, https://www.state.gov/joint-statement-on-improving-east-micronesia-telecommunications-connectivity/

[4] Invisible and vital: undersea cables and Transatlantic security, Center for Strategic and International Studies, 11 June 2021, https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

[5] Security threats to undersea communications – cables and infrastructure – consequences for the EU, Policy Department for External Relations, European Parliament, June 2022, https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

[6] Bridging the digital divide in the Pacific, Fiame Naomi Mata'fa, 5 April 2023, https://www.aspistrategist.org.au/bridging-the-digital-divide-in-pacific-island-states/

To build a more resilient region, Australia should continue to fund and co-fund strategic submarine cable projects in the Indo-Pacific, as recommended by security policy experts, working together with countries such as Japan, US, India, the UK, and the EU.[7] A recent National Security College report suggested that Australia should also consider co-funding new submarine cables in the Indian Ocean working collaboratively with India and France.[8] These critical connections are a vital enabler for improved cyber resilience as well as economic and national security in our region. By improving the cyber security and resilience of our partners, Australia can also strengthen our own cyber resilience.

We recognise that the small markets in the Pacific Islands limit commercial incentives to invest in infrastructure. Australia should use its emerging position as an Indo-Pacific cable hub by partnering with private-sector operators to extend cable infrastructure to underserved nations throughout the region. This partnership could include funding the inclusion of branching units on commercial cables as they are being planned. These branching units could later be used to deliver cable spurs, pending negotiations with the countries they are proposed to connect.

Vocus submits that the Government should continue to build on its successful role in co-funding the Coral Sea Cable System, which connects Port Moresby in Papua New Guinea and Honiara in the Solomon Islands to Sydney. This project was long overdue as high-speed internet was not available to the overwhelming majority of Solomon Islanders. Prior to the project, the Solomon Islands was dependent on expensive satellite links which provide limited bandwidth and low speeds compared to fibre infrastructure.[9] The project increased available data capacity to the Solomon Islands by 6,000 times. The Coral Sea Cable system was majority funded by Australia and with our extensive experience and expertise in fibre optic networks and delivery of large-scale submarine cable projects, Vocus was chosen to design and deliver the project, with the system being completed in December 2019.

**Secure and sovereign data storage and processing**

Australia also has the opportunity to leverage its well-established data centre infrastructure and cloud services industry to be utilised by our Indo-Pacific neighbours. Similar to submarine cables, smaller Pacific Islands nations are unlikely to attract commercial investment in data centres, which is where cloud services are housed. A lack of in-country datacentre infrastructure will stymie the development of online Government services (as well as commercial services such as online banking etc.), and an under-developed datacentre industry - lacking necessary investments in security - could increase cyber risks.

Rather than seeking to develop their own in-country datacentres, Pacific Islands nations could utilise Australian datacentres to host their own Government data and online services. Under the *Hosting Certification Framework,* Australia has established high security standards for the storage and processing of Government and citizen data, which could be made available to countries with underdeveloped datacentre infrastructure. To ensure that these nations maintain sovereignty over their data, Australia should seek to develop a legal framework which would allow this data to be stored and processed in Australian datacentres with strong legal protections preventing any access to such data by anyone other than the nation which 'owns' the data.

This approach could be conceptualised as a 'Data Embassy', where data belonging to the Governments of Pacific Islands nations and stored in Australia is provided with similar legal protections as their physical Embassies (or High Commissions). The security of data held and processed in Australian 'Data Embassies' would also be dependent on the data being transmitted between these nations and Australia via secure, sovereign submarine cables.

---

[7] Options for safeguarding undersea critical infrastructure, Australia and Indo-Pacific submarine cables, Samuel Bashfield and Anthony Bergin, Policy Options Paper No 25, June 2022, https://nsc.crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2022-06/nsc_pop_undersea_critical_infrastructure_no.25_web-1.pdf

[8] Submarine Cable Security in the Indian Ocean, National Security College Report, https://nsc.crawford.anu.edu.au/department-news/20995/submarine-cable-security-indian-ocean

[9] Case Study - Coral Sea Cable System, Global Infrastructure Hub, 30 November 2020, https://www.gihub.org/connectivity-across-borders/case-studies/coral-sea-cable-system/ accessed 3 April 2023

*What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?*

Cyber security includes protecting the confidentiality, availability, and integrity of computer systems and networks. A robust approach involves considering the specific threats at each layer of the stack, including the infrastructure by which data is transmitted. In October 2020, the NATO Secretary General, stressed the "crucial importance" of undersea cables, their role in strengthening resilience and the importance of being able to protect this infrastructure.[10] The implications of disruption to submarine cables are significant. Vocus submits that submarine cable protection should be considered as part of Australia's cyber security strategy.

The most common cause of damage to submarine cables is human error and negligence. Activities that pose the greatest threat are sea-bottom trawl fishing, dumping, sand dredging, and anchoring. According to International Cable Protection Committee statistics, fishing and anchoring accounts for approximately 70 per cent of global damage to submarine cables.[11] Such damage can stop the flow of voice and data to and from Australia.

The *Telecommunications Act 1997* allows the ACMA to declare a "protection zone" around submarine cables of national significance within Australian territory. One of the purposes of a protection zone is to provide enhanced security and protection for submarine cable(s) that lie within the limits of the zone by restricting or prohibiting activities that have the potential to damage cables.[12] Penalties for various offences committed within a protection zone provide a disincentive to activity that might cause cable damage.

The ACMA declared the three existing submarine cable protection zones over submarine cables of national significance of its own initiative in 2007 – two in Sydney and one in Perth. The need for these zones was identified by the Government and funding made available to the ACMA to establish these zones.

There have been no amendments to these protection zones, nor any new zones declared, since 2007. Sydney and Perth are no longer the only points where cables land – there are now landings in Darwin, Port Hedland, and Maroochydore; with proposals to land cables in Melbourne and Brisbane.

A wider distribution of cable landing points has distinct advantages for resiliency, and more should now be done to protect this current and planned nationally-significant infrastructure. For example, Vocus' North West Cable System has landings in Darwin and Port Hedland, neither of which have protection zones declared. This cable is currently being extended from Port Hedland to connect to the Australia Singapore Cable, which will complete the Darwin-Jakarta-Singapore Cable system, providing direct international connectivity into Darwin. This will act as an alternative international route to Perth or the east coast of Australia, and unlocks Darwin as a major new data hub for the Asia-Pacific. This new cable segment is due for completion in mid-2023.

Other operators have also announced plans for cable landings in Darwin, including the Hawaiki Nui cable connecting New Zealand, Australia, Indonesia, Singapore and the United States; and the Inligo Networks Asia Connect Cable-1 (ACC-1) connecting Indonesia-Singapore-Dili-Darwin-Japan-Guam and the USA.[13]

Vocus submits that the Government should make funding available to the ACMA to initiate the declaration of cable protection zones for the existing cables of national significance in Darwin, Port Hedland, and proposed cables landing in Melbourne and Brisbane.

---

[10] Online press conference by NATO Secretary General Jens Stoltenberg, 20 October 2020 https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en

[11] Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables' United Kingdom: International Cable Protection Committee, updated 18 November 2022, https://www.iscpc.org/publications/icpc-best-practices/

[12] Declaring a submarine cable protection zone, Guide for Applicants, ACMA, February 2022, https://www.acma.gov.au/sites/default/files/2022-02/Declaring%20a%20submarine%20cable%20protection%20zone_applicant%20guide.pdf

[13] Invest NT, Regional headquarters, digital connectivity, https://invest.nt.gov.au/investment-opportunities/regional-hq-attraction (accessed 31 March 2023)

The efficacy of the cable protection zone regime relies on shipping operators being aware of the zones. Education for all stakeholders who operate near critical submarine cable infrastructure is therefore essential. As various parties have submitted for more than a decade, the cable protection zones play a necessary but insufficient role in protecting submarine cables.[14]

We submit that the Government could do more to proactively educate and effectively monitor the protection of cables within Australian waters. In the ACMA's report on the operation of the submarine cable protection zone regime in 2010, all cable owners and operators that responded to the consultation suggested that active monitoring should occur.[15] As a first step, the Government should fund a study to determine cost effective approaches to compliance monitoring in protection zones to ensure the security of submarine cables.

Internationally, it has been noted that New Zealand has improved on Australia's regulatory approach to cable protection, as "unlike Australia, New Zealand has taken a proactive approach to enforcing prohibitions related to the zones."[16] New Zealand's Ministry of Transport in its public information about protecting undersea cables highlights that some cable protection areas "are patrolled by ship and helicopters 24/7 with protection officers and Maritime Police, so offenders are likely to get caught".[17] The proactive monitoring of the protected areas by sea and air patrols is also highlighted in other publications and educational campaigns including "catch fish - not cables!" notices.[18]

*What can the Government do to improve information sharing with industry on cyber threats?*

Vocus welcomes the Government's announcement of the establishment of a Co-ordinator for Cyber Security and the aim to ensure a centrally coordinated approach to Government's cyber security responsibility.

The new Co-ordinator for Cyber Security could also explore ways to work with industry to enhance gathering and sharing of information relating to submarine cable threats.

Domestic cyber security is closely linked with the resilience of our neighbours. Pacific leaders have called for an increasing emphasis on regional co-operation to address cyber security threats.[19] Australia should continue to work with our neighbours to build their national capabilities, including through our membership of the Pacific Cyber Security Operational Network. For example, a recent National Security College report recommended that Australia, India, and France could take a leading role in working with more vulnerable states in the Indian Ocean on developing procedures for information sharing on suspected cable attacks and anomalies.[20]

Please direct any questions regarding this submission to:

**Luke Coleman, Head of Government and Corporate Affairs,** [redacted]

[14] Australia's vulnerable submarine cables, ASPI The Strategist 31 May 2013, https://www.aspistrategist.org.au/australias-vulnerable-submarine-cables/

[15] Report on the operation of the submarine cable protection regime, ACMA, September 2010, https://apo.org.au/sites/default/files/resource-files/2010-09/apo-nid23392.pdf

[16] Policy Proposals for the United States to Protect the Undersea Cable System, Journal of Law, Technology & the Internet, Vo 13, No 1, 2021-2022, Kevin Frazier https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1133&context=jolti

[17] Protecting New Zealand's undersea cables, Ministry of Transport,https://www.transport.govt.nz/about-us/what-we-do/queries/protecting-new-zealands-undersea-cables/ (accessed 3 April 2023)

[18] Annual NZ Notice to Mariners, https://www.linz.govt.nz/sites/default/files/cust/hydro_almanac_ANTM-13_202223.pdf accessed 3 April 2023

[19] The Pacific Security Outlook Report, 2022-2023, Pacific Islands Forum, https://www.forumsec.org/wp-content/uploads/2023/01/Pacific-Security-Outlook-Report-2022-2023.pdf

[20] Submarine Cable Security in the Indian Ocean, National Security College Report, https://nsc.crawford.anu.edu.au/department-news/20995/submarine-cable-security-indian-ocean