Re: PJCIS - Telecommunications Act 1997, Section 313(1A), (2A)

Author: Paul Wilkins

Date: 22 January 2021

There is no clear meaning of "do their best" as required per Sections 313(1A) and (2A) of the Act. This is an artefact of a gap in the development of goals for national security policy, where there exists a serious gap between what's currently perceived as best practice, and where national security policy will need to be to combat threats into the future, to national carriage network infrastructure, and to essential network services of national importance.

To be brief, in both policy formulation, and the subsequent derivative legislation, there ought to be made an explicit distinction between endogenous carriage (carriage within national borders) and exogenous carriage (carriage that crosses international boundaries), and recognition/definition of "A National Carriage Boundary" to serve as a demarcation zone between endogenous and exogenous carriage networks, and for the application at the demarcation zone, of a standard and well defined National Carriage Security Profile on exogenous traffic flows.

The explicit recognition of this distinction would then be able to inform policy. The first consequence of such a recognition would be to create an architectural separation between endogenous and exogenous carriage, where exogenous carriage is explicitly recognised as having no security posture, while endogenous carriage has a recognisable and uniform security profile, defined by policy and legislative instruments. There should be statutory obligations on carriers to ensure that exogenous traffic flows align with the National Carriage Security Profile.

The distinction of carriage as either endogenous or exogenous, would then establish a demarcation zone at the national boundary, where national carriage security policy is imposed on exogenous traffic passing into or out of the national borders. This would facilitate valuable outcomes, including security at scale for national carriage networks and essential network services, the imposition of national jurisdiction on exogenous traffic flows, efficiencies of scale in addressing existential threats to the national carriage infrastructure, and creating the necessary framework, architecture, policies, and processes for cooperation and collaboration amongst exogenous carriers, and between them and government/security agencies.

Despite the merits of asking that carriers do “their best” to protect national networks as provided under Sections 313(1A) and (2A) of the Act, “their best” is subject to arbitrary definition and the individual interpretation of each carrier, preventing the development of uniform standards, architecture and processes. This is recognisable, for instance, in the “Clean Pipes” initiative, where some carriers are taking it on themselves because there is a lack of national policy. But the development of such initiatives is subject to the brand alignment of enterprise carriers vying for competitive advantage. Cooperation between carriers on the basis of a “best effort” obligation, cannot be effective or scalable. What is required is national policy and standardised architecture and processes to create a baseline security profile that applies across the national carriage network, and this requires the imposition of a national security posture at the endogenous/exogenous carriage interface, the “National Carriage Boundary”.

Furthermore, it may be actually impracticable under the present framework for exogenous carriers to mitigate certain risks to infrastructure and services, even if they were of a mind to address the risk. Owing to Australia’s rather unique geography as an island continent, the “National Carriage Boundary” is essentially an aggregate network of submarine cables. Due to existing commercial arrangements, carriers may have little architectural or operational control of the distal ends of submarine cables, operated and maintained by commercial partners, and because these locations are offshore, not subject to Australian jurisdiction. Recognition of a “National Carriage Boundary” and the definition of a National Carriage Security Profile would be able to inform future commercial arrangements and architectural development of distal submarine cable head ends.

Once given recognition of the National Carriage Boundary, policy should address potential threats to this essential infrastructure. For instance, one possible disaster scenario of concern to those shaping national carriage security, would be the failure of significant domestic cloud data centre(s), where an aggregate of service providers have a primary location in an Australian cloud data centre, but they have all opted for an offshore backup data centre location. A failure of the domestic primary data centre would give rise to an en mass relocation of Australian based services to offshore data centres, resulting in significant additional bulk traffic flows needing to be carried across the National Carriage Boundary. If these links were to saturate, national carriage services would be significantly impacted. Responsibility for addressing such a scenario rests squarely with government, where no exogenous carrier acting on their own initiative is capable of mitigating such a risk, even if they were of a mind to. Furthermore, cooperation amongst exogenous carriers is better able to spread the risk, but only where mechanisms for coordinated cooperation exist.

One approach might be for the Critical Infrastructure Centre to act as a point of coordination between exogenous carriers and the security agencies to ensure a consistent security profile applies at the National Carriage Boundary.

Extant Gaps in National Carriage Security Infrastructure

	Present State	Goal Architecture
National Carriage Boundary	No clear demarcation between exogenous and endogenous carriage networks	Establishment of a National Carriage Boundary, to serve as demarcation between endogenous and exogenous traffic
Standards	Best effort (per 313(1A)) as interpreted by carrier – arbitrary, heterogeneous, and unscalable	A single National Carriage Security Profile, to be adopted across all exogenous carriers, to be applied to exogenous traffic flows
Jurisdiction	No clear demarcation between exogenous and endogenous carriage	Imposition of sovereign jurisdiction on exogenous traffic flows via legislative instruments at the National Carriage Boundary
Architecture	Ad hoc across carriers and unscalable	Standardised baseline architecture for the National Carriage Boundary
Process	Ad hoc across carriers and unscalable	Established standardised mechanisms for exogenous carrier engagement
Cooperation	Ad hoc across carriers and unscalable	Standardised processes for intercarrier cooperation and liason with security services Standardised processes for the evolution of the National Carriage Boundary architecture
Essential Network Services - Bulk Carriage (protection against DDoS etc) - BGP routing - Domain Name Service (DNS) - Public Key infrastructure - Cloud Services (compute and offline storage)	Heterogeneous enterprise level protection Unscalable No specific mechanisms for protection of essential network services from exogenous sources	Established architecture, policy, and standardised processes for protection of essential network services at the National Carriage Boundary
National Carriage Boundary bulk flow capacity	Ad hoc across carriers Carrier security mechanisms don't address wider threats to the National Carriage Boundary	Established architecture, policy, and standardised processes for risk management of threats to bulk carriage across National Carriage Boundary