NSW Government Submission

ACCC Regional Mobile Infrastructure Inquiry

August 2022

Introduction

The NSW Government thanks the Australian Competition and Consumer Commission (ACCC) for the opportunity to provide a submission to the Regional Mobile Infrastructure Inquiry.

Regional NSW hosts a third of the state's population and produces around one fifth of the Gross State Product. Digital connectivity remains a crucial issue in supporting regional NSW to remain socially connected and is an investment priority under the Government's 20-year Economic Vision for Regional NSW. The impacts of COVID-19, the 2019-20 bushfires, and the 2022 flood events have highlighted the need for better connectivity across regional NSW to support both public safety and social and economic inclusion.

The NSW Government supports co-contribution programs to facilitate services and infrastructure co-location, such as the neutral host model and the active sharing model suggested in the consultation paper provided by the ACCC. This has significant potential to improve mobile coverage, competition, and consumer choice in regional areas, and provide economic efficiencies and incentives for telecommunications carriers operating in the regions.

The NSW Government is exploring active infrastructure sharing through the Mobile Coverage Program's Active Sharing Partnership. This new initiative seeks to establish collaborative partnerships between the telecommunications sector to design and deliver Mobile Coverage Solutions that use Active Infrastructure Sharing to deliver new and improved mobile coverage in regional NSW. The NSW Government will continue to advocate for policy, regulatory, and legislative reform necessary to facilitate greater and more reliable access and connectivity in regional and remote areas.

The NSW Government considers that 'emergency roaming' would provide an important safety measure, as recognised in the NSW Government submission to the 2021 Regional Telecommunications Independent Review and the Bushfire Inquiry Report. Emergency roaming would also complement other important initiatives being pursued by the NSW Government – such as our investment in *Public Safety Mobile Broadband* – to improve public safety and community resilience through improved access and connectivity for emergency services organisations.

Government investment should support competition and consumer choice

The Commonwealth has partnered with state governments to deliver various programs and initiatives aimed at improving mobile coverage in regional communities, and especially for remote or natural disaster-prone locations. While outside the immediate scope of this inquiry, the NSW Government has placed on record its position that future government investment and policy decisions relating to regional digital connectivity should drive competition and consumer choice.

There is an overwhelming need for further government support to address lack of mobile coverage in crucial areas such as small population locations, road corridors and visitor economy locations, fringe locations, and areas with low levels of market competition and consumer choice. There is only one Mobile Network Operator (MNO) in some regional and remote population centres.

Governments need to identify these gaps and make grant programs more competitive and more strongly focussed on delivering consumer choice outcomes to address the challenges with sharing of mobile infrastructure and provision of roaming services at competitive prices to the end customers.

Overview of key issues addressed in submission

This NSW Government submission addresses the issues raised in the Inquiry's discussion paper in two parts. Part one relates to access to towers and associated telecommunications infrastructure (questions 1-21). Part two deals with mobile roaming during natural disasters and other emergencies (questions 22-30).

Key comments on each part are summarised below.

Access to towers and telecommunications infrastructure

- The NSW Government supports infrastructure sharing models to achieve improved coverage and better outcomes for end users in regional areas.
- Inadequate private investment in 5G in regional areas will contribute to increasing the digital divide.
- The NSW Government is doing its part to improve regional connectivity through programs such as the Mobile Black Spot Program and the Regional Digital Connectivity Program, as well as our NSW Government Connectivity Strategy which will investigate innovative opportunities to improve regional connectivity.
- Data sharing around carrier infrastructure is vital to enable emergency services organisations to keep telecommunications infrastructure safe, especially during natural disasters. This includes the NSW Telco Authority's Telecommunications Emergency Management Unit (TEMU).
- Regulatory mechanisms under the *Telecommunications Act 1997* or the *Security of Critical Infrastructure Act 2018* are needed to support improved data provision and resilience measures.

Mobile roaming during natural disasters and other emergencies

- Loss of telecommunications, including triple zero calls, significantly reduces the capacity of emergency services organisations to respond to emergencies and natural disasters, and the ability of community members and volunteers to access support and essential services.
- Mandatory temporary roaming during emergencies ('emergency roaming') for basic text, voice, and data services is needed for all citizens to provide an important safety measure that can help mitigate disruption caused by damage to telecommunications infrastructure.
- Emergency services require mandatory continuous (24/7) roaming available as a key part of Public Safety Mobile Broadband. This will support the resilience of emergency services organisations' communications during both business-as-usual activities and when preparing and responding to natural disasters and major events. 'Emergency roaming' is not sufficient to meet this need.
- The functionality of any emergency roaming needs regular testing to ensure it is reliable and immediately available when activated. While not within the scope of this inquiry, the introduction of continuous domestic roaming could offer a means of mitigating this risk by more effectively facilitating operational readiness.

Part One – Access to towers and associated telecommunications infrastructure

Costs involved in operation of telecommunications in regional NSW *(see questions 1-9)*

Telecommunications operating costs in regional NSW vary between vendors. For example, some vendors include power costs while others may not. Across NSW Government different agencies are involved in the operation of telecommunications through the planning process, as landholders or as radio network operators.

Planning costs

Planning costs contribute to the overall costs of building towers and other telecommunications infrastructure. Streamlined planning pathways are likely to further reduce associated planning costs. For example, the Transport and Infrastructure SEPP (State Environment Planning Policy) (Division 21 Telecommunications and other communications facilities) contains various streamlined planning pathways for such infrastructure including:

- new towers on land in rural zones RU1, RU2, RU3, or RU4 as complying development
- towers or masts as development permitted without consent (when carried out by a public authority), and
- various infrastructure as exempt development (including the replacement of existing towers).

Costs associated with the use of Crown Lands for infrastructure sites

The NSW Government holds and manages Crown land on behalf of the community to deliver public value. One of the ways this occurs is through the re-investment of revenue from commercial use and access to Crown land back into the Crown land estate, including revenue from communications licences.

The current rental fee schedule is location-density based and includes provision for subsidies where needed to support access. Licensing arrangements also consider other requirements such as the need to secure additional consents if the land is subject to an Aboriginal land claim.

Costs associated with the use of National Parks land for infrastructure sites

The NSW National Parks and Wildlife Service (NPWS) charges annual fees for all telecommunications facilities located on reserved land. These fees are reviewed every five years and adjusted based on the market rental for communications facilities. Fees also vary depending on location and are adjusted with the Consumer Price Index each year. Currently, the fees are:

- primary users – between approximately $18,000 (sites in remote areas) and $32,000 (sites in regional areas), and
- co-users – between approximately $9,000 (sites in remote areas) and $16,000 (sites in regional areas).

NPWS also incurs operational costs in their capacity as a landholder over the lifecycle of communications facilities built on reserved land.

Costs incurred in assessing new proposals

Determining applications under the *Environmental Planning and Assessment Act 1979* (NSW, '*EP&A Act')* can involve substantial time and resources. New telecommunications facilities can only be approved for construction on reserved land after the assessment of:

- the environmental impacts of the facility, in accordance with the EP&A Act, and
- the statutory criteria set out in section 153D of the *National Parks and Wildlife Act 1974* (NSW).

For example, determining an application for a new tower or co-user facility typically includes site visits with proponents, reviewing expert reports on the environmental and Aboriginal cultural heritage impacts and assessing bush fire risk mitigation measures required under the *Rural Fires Act 1997* (NSW). These tasks require input from operational and property staff, and mapping experts.

Costs involved in managing ongoing use of facilities

Many communications sites on NPWS land are accessed via NPWS's fire trail network – unsealed trails used for park management and fire-fighting purposes. These trails must be maintained to minimise environmental impacts, particularly erosion and drainage.

Use of these trails by telecommunications operators increases maintenance and compliance costs for NPWS. Given the remote locations of many of these sites this is a resource-intensive process.

- significant damage can be caused to trails if users don't comply with restrictions on vehicle size limits or on wet weather access
- users failing to follow access protocols resulting in other users being locked out or trails being unlawfully accessed by the public, and
- increased vehicle and personnel traffic into these remote locations increases the risk of spreading weeds.

Asset Protection Zones are also often required around communications facilities, in accordance with the Rural Fire Service's (RFS) Telecommunications Towers in Bush Fire Prone Areas – Practice Note 1/11. This involves routine maintenance and vegetation clearing.

Under the terms of licences granted by NPWS for communications facilities, telecommunications operators are liable for contributing to the costs of carrying out trail and APZ (Asset Protection Zone) maintenance. To date, NPWS has borne most of these costs but is currently transitioning to a cost-recovery model which will see all site users share the costs of trail and APZ maintenance.

Costs of maintaining Police Force Radio Networks

NSW Police Force (NSWPF) is currently a large Ultra High Frequency (UHF) radio network owner and operator. This requires installation of NSWPF Radio network equipment on carrier related structures. Carrier owned sites and carrier real estate managed sites are typically more expensive to utilise. From a NSWPF perspective, use of carrier sites are often seen as too expensive and sometimes cost prohibitive.

NSWPF spend approximately $3 million per year overall on outgoing site rental related costs for housing NSWPF radio network equipment on third party structures to landowners and facilities. These costs are a mix of mobile phone carrier and non-carrier related costs.

Access to carrier owned sites and carrier managed sites have complex processes for site applications and site changes.

In most cases, NSWPF as an emergency services organisation is charged a lower rate than carriers, but there is a wide variation in costs charged by private versus public entities.

Commercial arrangements typically take the form of formal agreements that are drafted and reviewed by legal firms engaged by NSWPF. Arrangements are usually established as a head licence agreement covering multiple sites or multiple licence agreements. NSWPF typically engages in five-year terms with renewal options.

Costs of providing mobile infrastructure can be prohibitive for upfront and ongoing costs. In addition, there can be a loss of real estate in tower reservations, costs for power lead in and for structural upgrades and maintenance. The cost of co-locating varies in many locations.

Accessing towers and infrastructure

NSWPF has been operating a radio network for almost one hundred years and over this time has established relationships with various landowners and managers to house infrastructure.

Maintenance of access tracks to infrastructure is frequently overlooked as an issue. Weather events can wipe out physical road access to sites, with track restoration being expensive in some scenarios. Often there is no centralised maintenance process for one or multiple entities to contribute to costs. If considering infrastructure sharing models, models to share associated maintenance costs including managing access roads should also be explored.

There are many considerations when deciding whether to provide towers or access to towers including:

- the cost of building a new site versus using existing sites
- the availability of power, especially in regional areas
- structural status and integrity of the towers that are already available for use
- preservation of tower real estate by carriers for future technology use
- consideration of land use approvals which may be required under the *EP&A Act* and associated instruments, and
- Landing zones – while these are a relatively new concept, the ability to fly in assets, fuel, or support engineers to physically isolated sites may be attractive to emergency service organisations.

Note that it is not only access to towers that presents a risk to mobile network operations, but also backhaul. A recent failure caused by damaged backhaul fibre removed all telecommunications services within a region. Mobile coverage in the area was unavailable for several days, impacting communities, communications, and security within the region.

Implications of divestment of tower infrastructure by Mobile Network Operators *(see question 10)*

There is limited commercial incentive for MNOs to invest in new and improved mobile infrastructure in regional NSW, especially areas with low population densities. Commercial returns for carriers from locations without coverage are minimal as more attractive locations have been serviced or have received some form of public funding subsidy. Higher costs of infrastructure deployment and upgrades, limited consumer demand, and lower return on investment compared to metropolitan areas may mean that MNOs are unable to give remote areas the same level of priority. MNOs also prefer to invest in areas that provide continuous coverage with their existing networks. As a result, there are many locations which have no or poor mobile coverage in regional NSW.

There are emerging market dynamics associated with the recent divestment of tower infrastructure by MNOs, with potential risks that will need to be monitored carefully. Similar risks exist and have been effectively regulated in other utility sectors that have moved to separate service provision and asset management businesses.

Impacts of transition to 5G *(see question 19)*

5G networks will deliver faster speeds, better reliability, and improved capacity. In addition to bringing improved mobile experiences for consumers, 5G has a wide range of commercial applications. It is critical that regional businesses and consumers are not left behind and do not miss out on the utility of 5G. We are facing a critical phase of network development where regional coverage should not be diminished as spectrum is repurposed and networks upgraded to 4G and 5G as 3G services are decommissioned from 2024 onwards. This is also a crucial consideration in relation to emergency service communications during an emergency period.

In the context of speed and latency, the current focus of operators planning for 5G appears to be directed towards high-density areas, with expansion into regional areas a lower priority. As 5G will be increasingly relied upon for use-cases for new products and services the digital divide will be further widened unless 5G becomes more widespread in regional areas.

Part Two – Mobile roaming during natural disasters and other emergencies

Temporary mobile roaming *(see questions 22 and 23)*

The NSW Government welcomes the inquiry into the feasibility of temporary mobile roaming services to be provided during natural disasters and other such emergencies (‘emergency roaming’). This was recommended in our submission to the Review and in the NSW Bushfire Inquiry’s final report (Recommendation 30).

As submitted to the Review, the NSW Government strongly supports the implementation of mandatory domestic roaming on commercial mobile networks for emergency-related communications from within affected communities and areas.

Separate consideration should also be given to expanding existing emergency call service (triple zero, 112, and 106) obligations to for customers to be able to make voice calls to additional numbers such as 131 444 (Police Assistance Line), 132 500 (State Emergency Service, SES), and 1800 679 737 (NSW Rural Fire Service (RFS)) at all times and from any location where there is any available network.

Family members, friends, neighbours, community members, and volunteers play a significant role in protecting each other and property during natural disasters and major emergencies. They are often the closest available responders and their efforts are highly valuable, particularly when the required actions do not necessitate an emergency services organisation response. This also allows emergency services organisations to remain focussed on high priority operations, particularly at times when their resources are likely to be stretched by potentially multiple emergency events. This does not diminish or substitute the primary role of emergency services organisations and triple zero emergency calls but augments the wider response effort when it is safe and appropriate to do so.

For example, a neighbouring farm may have a tractor that could assist with expanding a firebreak, a friend’s boat could move livestock to higher ground from a flooded property, or a local nurse may provide medical treatment that does not require the attendance of an ambulance or hospitalisation. Communications between those in need and those able to assist are essential in these circumstances.

Direct communications between emergency services organisation members and volunteers and community members also play a key part in emergency response efforts. For example, volunteers with official roles in emergency service organisations may rely on mobile phone calls, SMS, and paging to receive instructions about where and when to deploy in emergency response efforts. Additionally, a locally based NSW SES or NSW RFS member acting in an official capacity may seek to contact local community members, also being their neighbours, to provide updates or conduct welfare checks and confirm their location and situation. Depending on which networks individuals are subscribed to, and which are available, such direct communication may not be achievable without emergency roaming.

Similarly, the timely access to rapidly changing information is critical during emergencies and natural disasters. This includes access to data from applications such as the NSW RFS’ ‘Fires Near Me’ app, local status updates, and information that rely on communications networks to be accessible.

Emergency service organisations generally have access to comprehensive private mobile radio network coverage to support emergency responses, however, increasingly there is a requirement for broadband data that is not able to be met by these existing networks. Access to corporate systems (including from mobile data terminals and smart devices) and streaming video may result in improved operational outcomes.

Possible limitations to emergency roaming include:

- capacity and data throughput caps before sites become contended and unusable
- billing complexities whilst roaming
- spectrum and band limitations offered by some carriers at some locales may not permit the correct functioning of all devices, and
- individual device APN configurations to facilitate alternate network connections could be problematic.

Risks to the effectiveness of emergency roaming *(see questions 24, 25, and 26)*

While the NSW Government supports temporary emergency roaming as a mechanism to improve connectivity and coordination during emergencies and natural disasters, there are also risks to its effectiveness that need to be appropriately managed.

The protocols and procedures for activation of emergency roaming must be sufficiently dynamic, and consideration must be given to the timeliness and mechanism for activating roaming. If roaming is not activated in a timely manner, it could potentially affect actions to preserve lives, property, and livestock.

Additionally, the functionality of emergency roaming should be tested regularly to ensure that it will be operational immediately when required. Even though continuous domestic roaming is not the focus of this inquiry, if this form of roaming were introduced, it would provide better surety that the functionality is regularly tested and that any issues are identified and corrected, thus reducing the chances of failure when the functionality is most needed during emergencies.

While technical requirements to enable temporary mobile roaming will largely be a consideration for carriers, there will be implications for government agencies such as NSWPF with their ICT systems, including the ability for APNs to be accessible across various networks and subsequent security considerations. It is crucial that any emergency roaming covers both voice and data, as social media is critically important for sharing multilingual emergency information.

Many risks relate to inherent issues that face carriers during emergencies due to being designed for day-to-day use and having limitations in network resilience. These include:

- physical loss of sites
- network congestion during major emergencies
- loss of mains power
- physical access not possible due to washed out or damaged access tracks limiting ability to restore sites, and
- technical faults triggered by multiple impacts to normal operating conditions.

Recent disaster events in NSW have highlighted that it is not the towers themselves that are most crucial in maintaining tower operations but the infrastructure supporting them. In both recent fire and flood events, significant damage to the fibre backhaul and loss of power have proved more significant obstacles than damage to towers. Consideration would also need to be given to the implications for emergency service providers in using the network if network congestion increased due to a greater customer base than a particular customer network was originally designed for. Priority access for emergency service organisations may help to mitigate this risk.

Further risks to the effectiveness of emergency roaming stem from the infrastructure models adopted by carriers in regional areas. Infrastructure sharing models, including neutral host, active sharing, and co-location agreements, provide opportunities for multi-carrier networks to operate in regional areas where they may otherwise not consider it to be economically viable. Therefore, we strongly support this approach. However, notwithstanding this support, such an approach also brings with it risks in terms of the potential benefits from emergency roaming. If some or all carriers are sharing the same site, and that site is adversely affected by a natural disaster, it could cause emergency roaming to be ineffective across all networks if all carriers are suffering outages at that site.

Protocols for emergency declarations *(see question 27)*

The authority, protocols, and procedures for enacting emergency roaming in a specific area for an emergency or natural disaster must be sufficiently dynamic and efficient to ensure their effectiveness. The relevant authority should therefore sit at the state/territory jurisdictional level, due to their primary roles and responsibilities for emergency management, and at an appropriate operational level to ensure efficiency of application.

All MNOs have Emergency Service liaison Officers that communicate with the NSW Government's TelcoFAC (Telecommunications Services Functional Area Coordinator) during critical events.

NSW Telecommunications Authority (TEMU)

Sub-sections 313(4A) (c), (d) and (e) of the *Telecommunications Act 1997* (Cth) (Telco Act) establish obligations for carriers and carriage service providers to give reasonable help to authorities of the Commonwealth, states, and territories if a national emergency declaration[1] or declared state of emergency[2] is in force. Agreement on the terms and conditions of such help is required between the carrier and relevant authority under section 314. These provisions could be used to facilitate emergency roaming. However, they rely on 'high-level' (Governor-General or Premier) emergency declarations, which may not be operationally effective or efficient in the circumstances, as such declarations are generally made in response to an event that has occurred or is continuing, leaving limited scope for pre-emptive action to facilitate connectivity, and prior communication and notifications.

A more practicable option could be to empower a suitably qualified and informed senior emergency management authority within each jurisdiction to authorise the enactment of emergency roaming at either of the 'stages of emergency' including preparation, response, and recovery.[3] This will require informed consideration of the specific, prevailing circumstances before a decision or declaration is made. For example, an anticipated flooding event, based on weather predictions, or an approaching bushfire could constitute sufficient pre-emptive grounds to enact emergency roaming protocols.

Any decision to enact emergency roaming in NSW could be informed by TEMU, located within the NSW Telco Authority. TEMU has responsibility, under the *SERM Act* and EMPLAN on behalf of the TELCOFAC, for coordinating communications between commercial carriers and emergency services organisations for the protection of critical telecommunications infrastructure, the deployment of network augmentation and ensuring safe access to telecommunications infrastructure during emergencies and natural disasters. This includes the identification of telecommunications sites at risk from developing events, such as by tracking the direction of bushfires in relation to telecommunications sites. This occurs from its Telecommunications Operations Centre, the State Emergency Operations Centre and other locations to which TEMU members are deployed during emergency management operations.

To execute its functions, TEMU maintains close liaison with commercial carriers and other emergency management authorities, collects data and produces real-time event mapping to provide situational awareness updates to frontline responders.

[1] Under the *National Emergency Declaration Act 2020* (Cth).
[2] Under the *State Emergency and Rescue Management Act 1989* (NSW) in NSW and respective legislation in other states and territories.
[3] *State Emergency and Rescue Management Act 1989* (NSW), s 5 Stages of emergency.

Additionally, standard 'triggers' could be used to pre-emptively enact emergency roaming. For example, any area in which the Emergency Alert system has been activated, or when a 'catastrophic' bush fire day has been forecasted or declared, or other similar event-based alternatives could be established as triggers for this purpose.

Resilience measures *(see question 28)*

The frequency and severity of recent natural disasters and the reliance on access to telecommunications networks during response and recovery activities has led to a range of inquiry recommendations and governmental initiatives regarding network availability.

As part of its National Bushfire Response Package, the Commonwealth Government invested in activities for commercial network operators to improve regional network resilience at specific network sites. This includes the Strengthening Telecommunications Against Natural Disasters (STAND) package, with its Mobile Network Hardening Program and Mobile Black Spot Program funding used for generators, battery backup systems, transmission resilience and physical hardening against bushfires. These programs, and others, are supported by state government participation and project management.

Additionally, the Pathway to Infrastructure Resilience, released by Infrastructure Australia in partnership with Infrastructure NSW, provided guidance to support telecommunications resilience.

Such non-regulatory activities, undertaken in partnership with commercial network operators, offer improvements in network resilience but are limited in their adoption and application as they rely on the carriers to participate.

However, the implementation of regulatory measures to increase network resilience would ensure sites are appropriately hardened and increase the likelihood that they remain operational when needed most.

As communications infrastructure is categorised as 'critical infrastructure' under the SOCI Act, owners are required to adopt an all-hazards risk management approach to protecting their infrastructure. Such endeavours establish good practice and benchmarking opportunities for site resilience; however, they may be limited and not sufficiently prescriptive to achieve adequate resilience.

The development and implementation of communications site resilience standards, supported by regulation, would be highly advantageous for increasing communications network availability when sites may otherwise be at greater risk of failure, particularly during times of natural disaster events.

The SOCI Act's 'risk management programs' could include a requirement to meet stipulated resilience measures for telecommunications infrastructure, including, but not limited to redundant backhaul and on-site power backup.

Redundancy refers to the duplication of certain technical components on a site to ensure increased resilience and reliability of the network.

On-site power backup is usually in the form of battery backup, which should last for around 15 hours after electrical power loss and can be supplemented with solar power.

The resilience of telecommunications coverage could be improved through legislating requirements for commercial carriers to have on-site power backup and alternative sources of network coverage to enable continuity of critical mobile and data communications for citizens in a crisis where power failures occur.

Consideration could also be given to the following:

- methods for deploying temporary infrastructure as part of incident response
- establishing low-capacity long-range networks accessed only during disasters by the public and emergency services
- portable cell towers with multiple backhaul options under control of first responders would produce fast results
- use of mobile boosters and repeaters on government sites connected to networks via fibre
- enhanced detailed fault and carrier outage alerting (ideally a dashboard)
- all weather access to sites, and
- landing zones at mountain top sites to allow access during site physical isolations.

New Technologies can assist with communications capabilities during an emergency *(see question 30)*

Agencies across NSW Government have identified several emerging technologies that may assist with improving mobile coverage during emergency periods. Technologies which could be investigated further include:

- investment in deployables such tactical mobiles and establishing mechanisms for their use/deployment by emergency service organisations to augment coverage for use by the general public and emergency service organisations in blackspot locations
- self-healing publicly facing mesh networks, and
- emerging technology LEO satellites such as Starlink could be used to improve backhaul resilience and provide cost effective high bandwidth Data access that is not dependent on localized terrestrial Sites.

Temporary and continuous roaming for emergency services and Public Safety Mobile Broadband

While not directly in scope for this Inquiry, some of the requirements for the implementation of Public Safety Mobile Broadband (PSMB) in Australia may be considered in the context of the Inquiry's focus on 'emergency roaming', due to the similar nature and technical elements of their application.

PSMB is a mission-critical mobile data capability being adopted by emergency services organisations internationally. Australian jurisdictions have been working collaboratively towards implementation of a nationally interoperable PSMB network. The PSMB National Program Management Office (NPMO) is hosted by Emergency Management Australia and has a governance framework reporting up to the National Emergency Management Ministers Meeting (NEMMM).

While the design of Australia's PSMB solution is not yet complete, it is anticipated that it will involve the use of existing commercial carrier networks. The inclusion of multiple commercial carrier networks in a PSMB capability introduces redundancy, allowing communications to continue on an alternative carrier network if one network is not operational or is inaccessible.

This constitutes another form of network roaming and is similar to the use purpose of ‘emergency roaming’ for emergency affected communities that is a subject of this Inquiry.

However, in the case of PSMB, this roaming is reserved for the operational communications of emergency services organisations only. Its use would complement existing voice radio networks, such as NSW’s Public Safety Network, that emergency services organisations currently use to communicate as they perform their functions of protecting lives and property.

While critical during emergencies, PSMB roaming would not be limited to being enacted for a specific emergency in a specific location only but would instead be always operational and in all places to meet business-as-usual public safety requirements, in addition to its application for emergencies and natural disasters.

The NSW Government proposes that the ACCC considers the requirements for PSMB roaming in parallel with its research into the potential for emergency roaming, as any regulatory mechanisms for the implementation of both could be shared. The Commonwealth is currently undertaking a PSMB Strategic Review with objectives including providing advice, findings, and recommendations on ‘policy and regulatory settings required to establish and maintain a PSMB capability’. Hence, the ACCC’s Inquiry may benefit from consulting with the PSMB Strategic Review, which is required to deliver a final report to the Commonwealth Government by October 2022, on this issue.

Data sharing

There is considerable scope for emergency roaming to be complemented by improved telecommunications site data sharing. Data sharing can enable improved targeting of regional connectivity programs, including the mobile black spots program. It could also significantly improve the capacity of organisations such as emergency services organisations and the NSW Telco Authority, through its TEMU functions, to keep telecommunications sites operational during emergencies and natural disasters.

Implement a natural disaster information sharing framework

Many widespread failures of telecommunications networks are preventable. The likelihood and consequence of these failures are significantly reduced when government agencies know where the critical parts of the network are and can take measures to both protect the infrastructure and replicate the function of the infrastructure if it is damaged or destroyed.

NSW Government agencies (such as the NSW Telco Authority) have limited visibility of carrier network infrastructure, which significantly impacts on public safety efforts across the separate phases of emergency management. The NSW Telco Authority has met with telecommunications carriers over several years to discuss this issue and has received varied responses, ultimately resulting in inadequate data.

In August 2021, the Communications Alliance released its Telecommunications – Facilities Information Sharing Industry Guideline (G665:2021), which is a positive step forward for standardising the sharing of information between carriers and government. However, voluntary self-regulation is inadequate when it comes to an area as critical as emergency management. For example, some information sharing is 'optional', which could undermine the ability of emergency management agencies to protect lives and property in a crisis.

Emergency management agencies could respond faster to telecommunications failures if they had regulated access to carriers' data about telecommunications infrastructure in real time (with appropriate protections for sensitive data).

Regulatory considerations

The NSW Government has identified two possible options regarding regulatory mechanisms to support the continuity of regional communications networks during emergencies and natural disasters. These concern the sharing of operational status information by MNOs and activities to improve communications site resilience.

Option A suggests leveraging a 'designated disaster plan' under the Telco Act and Option B suggests utilising 'risk management programs' under the *Security of Critical Infrastructure Act 2018* (Cth, *SOCI Act*).

Option A – designated disaster plan

The *Telco Act*, under 'Division 4 – Disaster Plans', allows for the provision of a 'designated disaster plan' to cope with disasters and/or civil emergencies to be prepared by the Commonwealth, State or Territory (s 344). Section 345 allows conditions to be applied to carrier licences to comply with a designated disaster plan.

> *344 Designated disaster plans*
>
> *For the purposes of this Division, a designated disaster plan is a plan that:*
>
> > *(a) is for coping with disasters and/or civil emergencies; and*
> >
> > *(b) is prepared by the Commonwealth, a State or a Territory.*
>
> *345 Carrier licence conditions about designated disaster plans*
>
> *(1) An instrument under section 63 imposing conditions on a carrier licence held by a carrier may make provision for and in relation to compliance by the carrier with one or more specified designated disaster plans.*
>
> *63 Conditions of carrier licence declared by Minister*
>
> *Conditions applying to each carrier licence*
>
> *(1) The Minister may, by legislative instrument, declare that each carrier licence is subject to such conditions as are specified in the instrument.*

A designated disaster plan developed under s 344 of the *Telco Act* can be enforced via s 345 and s 63. Section 63 also allows for other conditions that can be applied to all carrier licences. The Minister could consider declaring conditions that designated disaster plans include measures for carrier site information and resilience measures such as redundant backhaul and on-site power backup.

Under Part 2, Division 3 of the *SOCI Act*, critical infrastructure owners are required to provide 'operational information' (s 7) and information relating to 'influence or control' (s 8A). This does not cover all the information that is needed by the NSW Telco Authority and other authorities to provide better security to those assets during natural disasters.

The information provided via a 'designated disaster plan' under the *Telco Act* could leverage and be in addition to information required of carriers (and other 'reporting entities') under the *SOCI Act*.

The Commonwealth might consider storing information provided under the *SOCI Act*, and that provided as part of a designated disaster plan in the same, secure location and to provide a format that allows carriers to provide the information in a single report or application.

It is also strongly recommended that a condition is applied to the carrier plans that information must be kept up to date. This could include a requirement for the provision of real-time operational status information if an outage or planned maintenance were to occur.

Resilience measures could also feature as a condition of all carrier designated disaster plans. This could include that, to satisfy s 344(a), certain standards must be met in relation to resilience of infrastructure. More information is included under ‘resilience measures’ below.

Although s 344(b) allows for a designated disaster plan to be developed by States and Territories, a Commonwealth plan would be a more efficient and consistent approach, affecting all carriers across Australia. A national plan would also have potentially fewer requirements and be more easily complied with by carriers than separate plans developed by each State and Territory.

Option B – risk management programs

With the communications sector now included in the definition of ‘critical infrastructure sector’ of the *SOCI Act* (s 8D), there is further potential to regulate obligations for critical infrastructure owners, including telecommunications networks, via critical infrastructure risk management programs.

Section 30AC of the *SOCI Act* requires any critical infrastructure owner to adopt and maintain a critical infrastructure risk management program. Section 30AH shows that some valuable information regarding management of risks and hazards to the asset must be included.

> *30AH Critical infrastructure risk management program*
>
> *(1) A critical infrastructure risk management program is a written program:*
>
> > *(a) that applies to a particular entity that is the responsible entity for one or more critical infrastructure assets; and*
> >
> > *(b) the purpose of which is to do the following for each of those assets:*
> >
> > > *(i) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;*
> > >
> > > *(ii) so far as it is reasonably practicable to do so—minimise or eliminate any material risk of such a hazard occurring;*
> > >
> > > *(iii) so far as it is reasonably practicable to do so—mitigate the relevant impact of such a hazard on the asset; and*
> >
> > *(c) that complies with such requirements (if any) as are specified in the rules.*

However, the information required at 30AH would need to be supplemented by additional information to adequately support the NSW Telco Authority and emergency services organisations to protect the infrastructure during a natural disaster or emergency that threatens the infrastructure. To enforce the provision of this information, the Minister may specify a requirement in the rules that further information is provided along with each critical infrastructure risk management program for telecommunications critical infrastructure.

Such requirements may then be implemented as carrier licence conditions under the *Telco Act*, to avoid regulatory duplication and provide clarity to the sector. This approach is consistent with that adopted by the Commonwealth for the recent obligations to register critical telecommunications assets and report cyber security incidents through the Telecommunications (Carrier Licence Conditions – Security Information) Declaration 2022 and the Telecommunications (Carriage Service Provider – Security Information) Determination 2022.

The information provided via a critical infrastructure risk management program could support and be in addition to information required of carriers (and other 'reporting entities') under Part 2, Division 3 of the *SOCI Act*. This would establish three sets of required information:

- 'operational information' and information relating to 'influence or control' required under Part 2, Division 3 of the *SOCI Act*
- real-time network operational status information, and
- site resilience information.

The Commonwealth might consider storing all three sets of information in the same, secure location and to provide a format that allows carriers to provide the information in a single report to reduce administrative burden on reporting entities and government.

Summary of regulatory options

The regulatory options above aim to ensure that carriers share information about the location and criticality of infrastructure and any plans in place to manage natural disasters, including resilience measures at telecommunications sites.

Information would be kept in a central, secure location and would be made available only to designated entities via a portal to ensure that the information is kept secure and viewed confidentially.

It is proposed to include a condition for carriers to provide both the 'Minimum Facility Data Sharing Information Set' and the 'Additional information' (to be made compulsory information) recommended by the Communications Alliance's Industry Guideline G665:2021 Telecommunications – Facilities Information Sharing (Guidelines).

Carriers provide some information on their facilities and assets as outlined in the 'minimum' and 'additional' (optional) data sets under the Guidelines. This data includes Radio Access Network architecture, transmission topology and interconnection points with other carriers.

NSW Telco Authority's TEMU uses this data to improve operational intelligence, assess potential risks to carrier assets during natural disasters and coordinate emergency responses to defend the assets and protect mobile communications that communities depend on during floods and bushfires.

Without legislative imperatives to provide this information, some carriers are reluctant to release some of the relevant data sets – particularly the additional data sets from the Guidelines – citing commercial and cyber security concerns. The NSW Telco Authority and

Spatial Services are in discussions with carriers and the Commonwealth's Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) and Home Affairs to address their information security concerns and source this data.

It is recommended that an approved legislative approach would:

- ensure that adequate information regarding critical telecommunications infrastructure is provided to enable improved protection of the assets and more reliable communications during natural disasters and emergencies
- require that the information is kept up to date
- require that the above information is provided to a secure portal managed by DITRDCA, and
- enable key agencies identified under the *SERM Act* as having a 'functional area' role to be able to access that information via the secure portal.

This proposal follows recommendations from the NSW Bushfire Inquiry 2020 and the Royal Commission into National Natural Disaster Arrangements 2020.