The Hon. Scott Morrison MP
Treasurer
Acting Minister for Home Affairs

Senator the Hon. Mitch Fifield
Minister for Communications and the Arts

JOINT MEDIA RELEASE

Thursday 23 August 2018

GOVERNMENT PROVIDES 5G SECURITY GUIDANCE TO AUSTRALIAN CARRIERS

Fifth Generation (5G) is the next evolution of mobile technology. It promises the ability to improve the daily lives of Australians, strengthen our connectivity and accelerate our networks.

5G will change the way people use, and rely on, mobile services, driving improvements in a range of ways for businesses and communities.

It will enable a new wave of innovation across our community and be used to connect other critical infrastructure, including electricity and water.

5G will underpin the development of smart cities and Internet of Things (IoT), and connect industrial control and safety of life systems, like remote surgery, and autonomous vehicles.

The Government wants to create an environment that allows Australian businesses to be at the forefront of seizing the benefits of 5G across the economy.

To achieve this, the Government is fostering a policy and regulatory environment to support a more efficient rollout, given its potential benefits to the economy.

The Government has undertaken an extensive review of the national security risks to 5G networks.

5G requires a change in the way the network operates compared to previous mobile generations. These changes will increase the potential for threats to our telecommunications networks, and these threats will increase over time as more services come online.

Acting Minister for Home Affairs Scott Morrison said the Government wants to realise the benefits of 5G but acknowledges that this new technology introduces additional risks.

“The security of 5G networks will have fundamental implications for all Australians, as well as the security of critical infrastructure, over the next decade,” Mr Morrison said.

Minister for Communications and the Arts Mitch Fifield said that it is vital that security and integrity underpinned the opportunities opened up by 5G networks.

“The Government is committed to the timely rollout of 5G networks in Australia. 5G will drive substantial economic and social benefits across the economy, through new technologies which will be used in autonomous vehicles, smart cities, and advanced agriculture,” Minister Fifield said.

The Government is committed to protecting this vital technology. To fully realise 5G’s benefits, Government and industry need to continue to work together to take necessary steps to safeguard the security of Australians’ information and communications at all times, and the integrity and availability of the networks themselves.

Last year, the Government introduced the Telecommunications Sector Security Reforms (TSSR) to provide a framework for Australia’s security agencies and industry to share sensitive information on threats to telecommunications networks.

TSSR introduces four new measures:

- a security obligation, which requires carriers and carriage service providers to protect their networks and facilities against threats to national security from unauthorised access or interference

- a notification requirement, which requires carriers and nominated carriage service providers to tell Government of any proposed changes to their telecommunications systems or services that are likely to have a material adverse effect on their capacity to comply with their security obligation

- the ability for Government to obtain more detailed information from carriers and carriage service providers in certain circumstances to support the work of the Critical Infrastructure Centre, and

- the ability to intervene and issue directions in cases where there are significant national security concerns that cannot be addressed through other means.

“The Government’s Telecommunications Sector Security Reforms, which commence on September 18, place obligations on telecommunications companies to protect Australian networks from unauthorised interference or access that might prejudice our national security,” Mr Morrison said.

5G requires a network architecture that is significantly different to previous mobile generations.

Traditionally, network equipment used by telecommunications operators has been categorised into the 'core' network and the 'edge' network.

The core network is where the more sensitive functions occur including access control, authentication, voice and data routing, and billing.

The edge consists of the radios and other equipment used to connect customer equipment (such as handsets, laptops and tablets) to the core network.

Where previous mobile networks featured clear functional divisions between the core and the edge, 5G is designed so that sensitive functions currently performed in the physically and logically separated core will gradually move closer to the edge of the network.

In that way, the distinction between the core and the edge will disappear over time.

This shift introduces new challenges for carriers trying to maintain their customers' security, as sensitive functions move outside of the highly protected core environment.

This new architecture provides a way to circumvent traditional security controls by exploiting equipment in the edge of the network – exploitation which may affect overall network integrity and availability, as well as the confidentiality of customer data. A long history of cyber incidents shows cyber actors target Australia and Australians.

Government has found no combination of technical security controls that sufficiently mitigate the risks.

While we are protected as far as possible by current security controls, the new network, with its increased complexity, would render these current protections ineffective in 5G.

Therefore, Government has expectations of the application of the TSSR obligations with respect to the involvement of third party vendors in 5G networks, including evolution of networks leading to mature 5G networks.

The Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference.

This applies equally to all carriers, consistent with government's long-standing commitment to a level playing field in the sector.

Carriers may still need to apply controls regardless of the vendor they choose. These controls would not displace existing cyber security practices or business risk mitigations.

Government is well positioned to address these risks in partnership with industry.

Mr Morrison said the Government has been working closely with telecommunications operators to ensure that they understand their new obligations and are ready to comply when the legislation commences on 18 September 2018.

“The Government has now provided carriers with clear guidance about how their new legal obligations apply to 5G networks.”

As 5G and related technologies continue to develop, new risks relating to the technology may emerge and require further Government consideration.

“The Government will continue to engage and support Australians, including the telecommunications industry, to manage national security risks,” Mr Morrison said.

“The Government’s first priority will always be the safety and security of Australians.”

Contacts: Treasurer – Andrew Carswell 0418 505 376, Kate Williams 0429 584 675
Minister Fifield – Geraldine Mitchell 0407 280 476, Guy Creighton 0438 815 302
The Hon. Scott Morrison MP, Sydney