Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

5G Telecommunications Security Guidance

Introduction

This guidance document is designed to assist critical telecommunications assets (previously known as carriers and nominated carrier service providers) understand the security risks associated with the deployment and operation of 5G networks and provides strategies to mitigate these risks. This document builds on the Government's 2018 5G Security Guidance, and while it explains the guidance in greater detail to assist entities with their regulatory obligations, it does not reflect a change in the Government's position on this issue.

Responsible entities are encouraged to maintain ongoing communication with the Telecommunications Security Risk section of the Cyber and Infrastructure Security Centre. If you are a representative of a critical telecommunications asset and wish to discuss this guidance, please contact telco.security@homeaffairs.gov.au.

Practical implications

To support compliance with regulatory obligations, responsible entities should, as best practice, conduct a risk assessment before engaging new vendors. In relation to 5G networks, this risk assessment should, among other considerations, assess whether a proposed or existing vendor may be subject to extrajudicial direction (EJD) that conflicts with Australian law. This should not be limited to particular vendors or countries of origin.

- The Government acknowledges that the global nature of telecommunications supply chains, and the concentration in market share for certain components, means that a degree of supply chain exposure to EJD may be unavoidable.
- The security risks to 5G networks are complex, and the Government has found that no combination of technical security controls will completely mitigate those risks. However, in relation to complying with the obligation to protect critical telecommunications assets from security risks, it is the Government's expectation that responsible entities mitigate security risks to the greatest extent possible.

To identify and mitigate security risk in 5G networks, responsible entities should conduct vendor risk assessments that consider:

- Possible exposure to EJD, including through the vendor's supply chain, manufacturing, development and support arrangements.
- The extent to which the vendor is able to ensure the security of the product or service they are delivering for the carrier.

Responsible entities should also conduct supply chain risk assessments whenever technology is introduced to their network that may impact their ability to meet their regulatory obligations, even if it is provided by an existing vendor.

- Consider if the vendor is providing a white label solution and selling third-party technology as their own.
- Consider the supply chains of a service or technology being offered by an existing vendor.

Outsourcing management of parts of an operator's network does not outsource the responsibility for effective control, which remains with the responsible entity.

Consistent with regulatory obligations, responsible entities (which may include operators of Mobile Private Networks [MPNs] that provide carriage services to the public) must notify the Department of Home Affairs whenever they intend to implement a change and they are aware that the change or proposed change to a telecommunication service or system is likely to have a material adverse effect on their capacity to comply with the obligation to protect their asset from all hazards, including security risks.

Working together to ensure 5G security

5G is a substantial driver for economic and social benefits across the economy. It is enabling a new wave of innovation across the Australian community and is being used to connect other critical infrastructure assets. 5G connectivity will underpin the development of smart cities and the Internet of Things (IoT), and connect industrial control and safety of life systems like remote surgery, and autonomous vehicles.

To fully realise 5G's benefits, Government and industry must work together to take necessary steps to safeguard the security of Australians' information and communication at all times, and the integrity and availability of the networks themselves. In 2018, the Government introduced a framework of regulation in Part 14 of the *Telecommunications Act 1997* (Tel Act), to formalise this information sharing between government and industry.

As of the 4th April 2025, as part of the legislative reforms to further uplift the security of the telecommunications sector, the existing obligations under Part 14 of the Tel Act have been moved into the *Security of Critical Infrastructure Act 2018.* This introduces new risk management obligations for some entities. The Government's policy and regulatory settings regarding telecommunications security are being reviewed on an ongoing basis to ensure they remain fit for purpose.

5G networks operate differently compared to previous mobile generations and the risk profile of 5G networks will increase over time as more services come online. The new 5G network, with its increased complexity, renders protections that were effective in 3G and 4G networks, ineffective in 5G.

The benefits offered by 5G are why its risk profile is significantly higher than previous generation mobile networks. It is vital that security and integrity are reinforced alongside the opportunities presented by 5G networks. More than ever, telecommunications networks are central to the functioning of vital services, and any disruption to the availability, integrity or confidentiality of networks could have potentially life-threatening consequences.

Features of 5G networks

5G requires a network architecture that is significantly different to previous mobile generations. Traditionally, network equipment used by telecommunications operators has been categorised into two networks: 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' network 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 are gradually moving closer to the edge of the network.

Because of this, the distinction between the core and the edge is disappearing over time. This shift introduces new challenges for carriers and carriage service providers trying to maintain network integrity and secure customer information, as sensitive functions move outside of the more protected core environment. This new architecture may allow traditional security controls to be circumvented by a malicious actor 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.

The security environment

Responsible entities should avoid complacency when it comes to security risks. Global trends are shifting constantly and an organisation's risk appetite and settings should be updated as necessary.

A long history of cyber incidents indicates that hostile cyber actors, including state-sponsored actors, have targeted Australia and Australians. In recent years, there have been significant data leaks caused by opportunistic cyber-attacks on critical infrastructure operators, including critical telecommunication assets. Therefore, Government has high expectations for responsible entities of critical telecommunications assets to take all reasonably practicable steps to protect their assets from all hazards, including security risks such as espionage or sabotage.

The Government considers the use of any vendor who may be subject to EJD could impact the ability of the carrier to adequately protect a 5G network.

Responsible entities may still need to apply controls regardless of the vendors they choose. These controls do not displace existing cyber security practices or business risk mitigations. As with all major changes to a telecommunications network, carriers need to conduct a risk assessment of any vendor technology that may impact the ability to meet regulatory obligations. This may include, but is not limited to, new vendors supplying critical elements of a telecommunication network or gaining access to customer information.

Any risk assessment should consider whether a vendor is subject to EJD and the vendor's ability to ensure the security of any solution being delivered. A risk assessment should also consider any support services being offered, including the location from where those services will be conducted, how they will be monitored, and how they will be logged and audited.

Where carriers outsource management of elements of their networks (including the management of data) to third-parties (such as Managed Service Providers), they must maintain a layer of control over the third-party in question, including the ability to unilaterally cut access, a log of all actions the third-party takes within host systems, and frequent auditing.

Operators of MPNs who provide carriage services to the public may be considered carriers and therefore have the same obligations to protect their critical telecommunications asset.

Entities operating 4G networks should also consider using this guidance to protect their networks from security risks.

Measures are vendor and country agnostic

Australia welcomes foreign investment in its telecommunications market, and takes a country-agnostic, transparent, risk-based and non-discriminatory approach to security regulation.

There is no list of vendors or countries to which this guidance applies. The onus is on network operators and carriers to conduct risk assessments, including supply chain risk assessments, for vendors that may be subject to EJD or any technology, software or service that may allow unauthorised access to a 5G network which could harm Australia's security interests.

Carriers have an obligation to submit notifications of certain changes and proposed changes to government, and where an internal risk assessment raises potential concerns, the importance of notifying government is amplified.

This process is not designed to be a roadblock to business development but a mechanism by which Government can offer guidance to meet regulatory obligations and mitigate risk.

Should there be any doubt as to the application of this guidance with regard to an element of a telecommunications network, either one that is already in place, or planned as a change, responsible entities are encouraged to submit a 'notification of change' to receive detailed technical guidance.