GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

TICSA Factsheet

New Zealand has legislation with regard to telecommunications network operators, designed to prevent, sufficiently mitigate, or remove security risks from the design, build and operation of public telecommunications networks. The Telecommunications (Interception Capability and Security) Act 2013 (TICSA) establishes obligations for New Zealand's telecommunications network operators with regard to network security. The Director-General of GCSB has a regulatory role for network security under Part 3 of TICSA. Since TICSA came into effect in 2014, the GCSB has received hundreds of notifications from network operators.

Network security is critical to New Zealand's national security

Given its pervasiveness and comparative ease of access, telecommunications infrastructure is a highly attractive target for states seeking to engage in espionage, sabotage, or foreign interference, or for criminal actors looking to exploit New Zealand businesses and individuals. Network security has therefore become a key area of concern for preserving New Zealand's national security, including its economic well-being.

Part 3 of TICSA was enacted to provide a mechanism for addressing these network security concerns. It applies to all network operators, regardless of size or customer base. TICSA promotes network operator and GCSB collaboration and cooperation on addressing network security.

The GCSB has set out service level targets for its consideration of notifications. Under those targets, GCSB endeavours to respond to all notifications within three working days and complete consideration of notifications within 20 working days.

Consideration of network security risks

The GCSB uses provisions of TICSA to assess potential network security risks, on a case by case basis. TICSA applies a country and vendor agnostic approach.

The GCSB uses information from a variety of sources in order to inform its view, including all relevant material provided by the network operator, as well as other available information about threats to network security, including information obtained from classified intelligence reporting.

In considering whether a network operator's proposal may give rise to a network security risk, the Director-General of GCSB must consider what the likelihood is that it will lead to the compromising or degrading of the New Zealand's public telecommunications network. The Director-General must also consider the likelihood of the impairment of the confidentiality,

availability or integrity of the telecommunications across the network. The Director-General must also consider the potential effect that could have on the provision of a prescribed list of services, including for example central or local government services and services within the finance and energy sectors.

If a network operator's proposal raises a more than minimal network security risk, and the network operator is unable to prevent or sufficiently mitigate this risk, the Director-General must decide whether to refer the matter to the Minister responsible for the GCSB. Before referring the matter to the Minister, the Chief Commissioner of Security Warrants reviews the Director-General's decision as to a significant network security risk. Once referred, the Minister may direct a network operator to take steps to prevent, sufficiently mitigate, or remove the significant network security risk. The Minister must have regard to different considerations from the Director-General's determination, including the potential consequences that the direction may have on competition and innovation in telecommunication markets.