

How does it Work? A Step By Step Guide

Disclaimer: This document is informational only and is not considered to be "Guidance" as defined in section 58 of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA)

This section sets out the steps for Network Operators and the GCSB in the network security process.

The Process

When a Network Operator is considering a proposed decision, course of action, or change to its network (i.e. a proposal) the Network Operator must consider whether it has to be notified to the GCSB:

- If it falls within an area of specified security interest (section 48 of TICSA), or
- The network operator becomes aware a network security risk may arise (section 46(1) of TICSA),
- And is not covered by an exemption (section 49 of TICSA).

If the proposal does not fall within an area of specified security interest, or is covered by an exemption, then no notification is required and the Network Operator can proceed with the proposal.

If it is unclear whether a proposal falls within the notification requirements of sections 48 or 46(1), or is covered by an exemption, for the avoidance of doubt, network operators should notify the GCSB.

If the proposal does fall within the notification requirements, then details of the proposal must be supplied to the GCSB.

The GCSB will consider whether the proposal would, if implemented, raise a network security risk. In doing so, the GCSB must consider the factors outlined in section 50(1) of TICSA.

If the GCSB considers the proposal will not raise a network security risk, Network Operators will be advised in writing and they may proceed with the proposal.

If the GCSB considers the proposal will raise a network security risk that is more than minimal GCSB will notify the Network Operator of that in writing. The Network Operator must not implement the proposal (section 51(1)(b) of TICSA).

- The GCSB will provide what information it can about the network security risk to the network operator in order to assist the Network Operator to understand the network security risk, dependent on the classification of the information and whether or not the Network Operator has security cleared representatives.

After being advised that a proposal will raise a network security risk(s), the Network Operator must, as soon as practicable, respond to the GCSB with a proposal to prevent or sufficiently mitigate the network security risk (section 51(3)). Alternatively, the operator could withdraw the notification.

The GCSB will assess whether the plan prevents or sufficiently mitigates the risk and will notify the Network Operator of the outcome in writing. To sufficiently mitigate means to reduce the risk to an acceptable level, and does not necessarily require that it be reduced to a minimal level, though that may be the only acceptable level with regard to some risks.

If the GCSB is satisfied that the plan prevents or sufficiently mitigates the network security risk(s) identified in the proposal, the Network Operator can implement the proposal, as long as the mitigation measures are also implemented (section 53 of TICSA).

If the Director-General, GCSB, is not satisfied that the mitigation proposal, or part of the proposal, will (if implemented) prevent or sufficiently mitigate the network security risk, the Director-General may decide not to accept the proposal or part of the proposal, and where the network security risk is significant, the Director-General of the GCSB must decide whether to refer the matter to the Minister responsible for the GCSB.

If the Director-General is considering whether to refer the matter to the Minister responsible for the GCSB, before referring the matter, the Commissioner of Intelligence Warrants must carry out a review to determine whether the significant network security risk identified by the Director-General exists or may arise. A copy of that decision will be provided to the Director-General and the Network Operator.

The Minister responsible for the GCSB may make a direction requiring the Network Operator to take steps to prevent, or sufficiently mitigate the network security risk. This process is explained later in this Guidance.

If the Director-General decides not to refer the matter to the Minister, the Network Operator will be notified in writing of this and can proceed to implement the proposal.

At any stage in the process, the Network Operator may withdraw the proposal.

Further detail

The GCSB can require Network Operators to provide information (section 78 of TICSAs). If further information is required under section 78, the Network Operator must provide it as soon as practicable after being notified it is required, but in any event within the timeframe specified, or if not specified, within 20 working days (section 79).

How we deal with your notification

Within the GCSB the TICSAs team have been assigned the role of handling notifications submitted by the Network Operators. A notification is submitted on the form that is provided on the NCSC website. The initial handling of a notification is to ensure that the necessary information required is provided by the Network Operator – the more complete the information provided, the swifter and more accurately the request can be handled.

This initial handling phase is usually completed in three days, and may include phone calls and emails to confirm details.

Once we have gathered enough information the team will send confirmation that the notification has been received and the team is in a position to assess the proposal in full.

The assessment is handled in the team by an assigned technical specialist. The assessment is peer reviewed within the team and should be complete within 20 days, usually much less.

Figure 1: The Network Proposal Process



