TICSA

Telecommunications (Interception Capability and Security) Act 2013

Guidance for Network Operators

www.gcsb.govt.nz
www.ncsc.govt.nz

Contents

Introduction

The following Guidance has been prepared to support the implementation and the on-going management of the network security part (Part 3) of the Telecommunications (Interception Capability and Security) Act 2013 (the TICSA).

It sets out the process established by the TICSA and is designed to assist network operators and the Government Communications Security Bureau (the GCSB) to work co-operatively and collaboratively with each other, so that network security risks can be identified and addressed as early as possible.

To ensure the network security process is implemented and operates in a pragmatic and practical way for the telecommunications industry, the GCSB will work together with network operators in an on-going dialogue based on good faith.

Network Operator or Service Provider?

A network operator (as defined in section 3 of the TICSA) is;

a) a person who owns, controls, or operates a public telecommunications network; or,

b) a person who supplied (whether by wholesale or retail) another person with the capability to provide a telecommunications service.

A service provider (also defined in section 3 of the TICSA) is;

a) means any person who, from within or outside New Zealand, provides or makes available in New Zealand a telecommunications service to an end-user (whether or not as part of a business undertaking and regardless of the nature of that business undertaking); but

b) does not include a network operator.

The Network Security provisions in Part 3 of the Act only apply to Network Operators as defined in the TICSA.

The TICSA was passed in November 2013 and relates to obligations on New Zealand's telecommunications network operators in two key areas – interception capabilities and network security.

Part 2 of the TICSA relates to a network operator's obligation to ensure public telecommunications networks are '**intercept capable**' to enable authorised government agencies to conduct lawful interception in accordance with their legal authority.

This Guidance does not deal with Part 2 (Interception capability duties) obligations. For guidance on interception capability obligations and registration, network operators should contact the New Zealand Police[1] who have released a separate guidance paper.

Part 3 of the TICSA relates to **network security** and outlines a framework under which network operators are required to engage with the GCSB about changes and developments with their networks where these intersect with national security.

The framework sets out a path to identify and address, prevent, mitigate, or remove the network security risks which may arise.

1 http://www.police.govt.nz/about-us/programmes-and-initiatives/telecommunications-interception-capability-security-act-2013

Section 7 of the TICSA;

Purpose of this Act relating to network security;

The purpose of this Act in relation to network security is to prevent, sufficiently mitigate, or remove security risks arising from—

(a) the design, build, or operation of public telecommunications networks; and

(b) interconnections to or between public telecommunications networks in New Zealand or with networks over-seas.

The TICSA (section 8) also sets out principles relating to network security that must, as far as practicable, be applied by both the Director and each network operator in relation to network security risks. Those principles are:

a) The principle that network security risks that might arise from a proposed decision, course of action, or change if implemented should be identified and addressed as early as possible:

b) The principle that the Director and each network operator should work co-operatively and collaboratively with each other in relation to the principle in paragraph (a).

Overview of the Guidance

This Guidance is issued by the Director of the GCSB under section 58 of the TICSA, to provide information about the requirements on network operators under the network security parts of the TICSA.

The Guidance does not replace the words of the TICSA itself, but is intended to give network operators more detail on what to expect and what is required from the process. It sets out the GCSB's understanding of the processes that will implement the TICSA's network security framework.

It is intended to inform network operators of their obligations and duties as they relate to network security under TICSA, in particular;

- identify the types of network proposal the GCSB requires notification of;
- identify the types of network proposal the GCSB does not require notification of;
- outlines the process by which the GCSB can grant exemptions to the duty to notify;
- outlines the process through which the GCSB will assess proposals and communicate responses; and
- establishes expected timeframes and information required to be supplied with a proposal.

This Guidance is not binding on network operators, however, in any court proceedings related to TICSA, compliance with the Guidance will be treated as evidence of compliance with the applicable requirements in the legislation (section 58).

The TICSA places the government's obligations in the network security process on the Director of the GCSB and so refers to "the Director" throughout Parts 3 and 4. A team in GCSB's National Cyber Security Centre (NCSC) is tasked to work on this process and they will be the primary point of contact available for network operators. For ease of reference, the Guidance refers to "the GCSB" when describing the duties placed on the GCSB's Director under TICSA.

This Guidance is the result of a process of consultation with network operators. The GCSB will continue to work with network operators on the use and development of the Guidance.

Any questions about the Guidance can be sent to: **ticsa@ncsc.govt.nz**

Focus of the network security part of TICSA: New Zealand's National Security

The focus of the network security part of the TICSA is the prevention, mitigation or removal of network security risks.

The GCSB will work with network operators co-operatively and collaboratively so that risks to New Zealand's national security, arising from the design, build or operation of public telecommunications networks and their interconnection to other networks both domestically and overseas, are identified and addressed.

Proposed decisions, courses of action or changes notified by network operators (called "proposals") are considered by the GCSB to identify whether they would raise a **network security risk**.

> *"Network security risk" has a specific meaning under TICSA, it is defined as;*
>
> > *"any actual or potential security risk arising from –*
> >
> > *(a) The design, build or operation of a public telecommunications network; or*
> >
> > *(b) Any interconnection to or between public telecommunications networks in New Zealand or with telecommunications networks overseas."*
>
> "Security risk" is also defined by TICSA;
>
> > *"it means any actual or potential risk to **New Zealand's national security.**"*

While "national security" is not specifically defined, for the purposes of the network security provision of the TICSA, its meaning is found in the list of factors that the GCSB must consider when deciding if a proposal presents a network security risk.

Section 50 is set out in full later in this Guidance, however in short, a network security risk requires consideration of the likelihood that the proposal will lead to;

- the compromise or degradation of the public telecommunications network;
- the impairment of the confidentiality, availability or integrity of telecommunications across the network; and,
- the potential effect of that on the provision of important services (including for example, central or local government services, health or transport services).

In some cases, a "network security risk" as defined above, may also be or overlap with a common security risk. The difference is in how that risk may be exploited by specific threat actors, and the impact that it may have on critical national networks and services.

The focus on New Zealand's national security in the Act means that the duty to notify under the TICSA is limited to:

- Proposals that affect parts of networks which are designated "areas of specified security interest" – these are the areas where these network security risks are more likely to arise (section 48 of the TICSA); and
- Situations when the network operator becomes aware of any network security risk that may arise if a proposal is implemented (in any part of the network) (section 46(1) of the TICSA).

It also means that any consideration of a proposal that is found not to give rise to a "network security risk" has only been reviewed in relation to New Zealand's national security, and not broader network security risks which a network operator might commonly consider (such as privacy, or commercial security controls).

The GCSB's consideration of proposals will not constitute an endorsement of the proposal in any broader security sense, and must not be considered as a substitute for standard business risk assessments, standard due diligence, enterprise security reviews or any other form of assessment that a network operator would usually perform when initiating a new project or change.

Similarly, while employing good information assurance practises supports the security of networks, the GCSB will not consider in its assessment adherence to 'information assurance' practices (which network operators would commonly use as part of their normal business practice) such as;

- adherence to international standards;
- privacy protection obligations;
- any duties required of network operators under New Zealand legislation (other than TICSA); or
- any other network security risk that does not involve a risk to national security.

Section 1:
What are the General Requirements?

Registration

Under Part 4 of the TICSA, network operators are required to register (section 60). The Register has been established, and is maintained by the New Zealand Police. A registrar has also been appointed. Information about the Register and the registration process is available from the New Zealand Police.

Network operators must be registered within 3 months from 11 February 2014 (or within 3 months after becoming a network operator). Once submitted, registration details need to be kept up-to-date with an annual review from November 2015.

If an organisation is uncertain whether they meet the definition of a network operator they should contact the Registrar. Enquiries about registration should be directed to New Zealand Police, which oversee the registration process.

Network operators can register by completing a form made available by contacting the Registrar through the **New Zealand Police website.**[2]

Security Cleared Personnel

To assist the GCSB and network operators to work together on network security risks, network operators may nominate a suitable employee (or employees) to apply for a SECRET level GCSB sponsored security clearance.

Network operators may also, upon request, be required to nominate an individual for security clearance (section 75).

Having cleared staff within network operators allows the GCSB to share certain information about network security risks that is classified. While these individuals cannot pass classified information to un-cleared colleagues, they will be able to give informed guidance on identifying and addressing network security risks.

If a network operator does not have cleared staff, the GCSB will still seek to engage with them, and share what information it can about network security risks.

As a guide when considering which employees to nominate to be cleared, network operators should consider;

- the position of those people within their organisation;
- the minimum number of people required to be cleared to respond if a network security risk is identified in a proposal; and
- whether the nominated employees hold sufficient technical knowledge to understand the nature of the risk conveyed.

Network operators should only nominate staff they believe are likely to obtain and maintain a clearance, and to nominate as few employees as possible to sufficiently support their organisation in fulfilling this function.

As a guide, nominated staff should be New Zealand citizens who have lived in New Zealand for at least 10 years.

2 http://www.police.govt.nz/about-us/programmes-and-initiatives/telecommunications-interception-capability-security-act-2013

To apply for clearance for the network security provisions of the TICSA, network operators should contact the GCSB via email to ticsa@ncsc.govt.nz with the following information about the nominated person:

- name
- date of birth
- whether they are a New Zealand citizen or permanent resident (if the latter, the date they arrived in New Zealand)
- company
- role within the company
- contact numbers
- email address

A representative from the GCSB will respond within 3 business days and suitable candidates will be referred to initiate the clearance process. It should be noted that the clearance process is not run by the GCSB, and may take a significant length of time. Candidates who receive their clearance will be notified in writing.

Section 2:
What and When to Notify

Network Operators Duty to Engage in Good Faith

> Section 46(2) of the TICSA;
>
> A network operator must act honestly and in good faith when engaging with the Director in relation to any matter in this Part [Part 3].

The obligation in section 46(2) to act honestly and in good faith is relevant for network operators and GCSB's engagement with each other throughout the TICSA network security processes. As a concept "good faith" is difficult to define in isolation and so is best understood by reference to duties in the TICSA.

For example, network operators would be acting in good faith when they consider and identify proposals that need to be notified, and do so with sufficient time for the GCSB to consider a proposal to determine whether it raises any network security risk. Similarly, a network operator notifying the GCSB of a network security risk they become aware of as soon as they have identified and considered it, is acting in good faith.

Good faith also underlines a network operator's obligation under s 46(3) to provide the GCSB with access to its employees, contractors or agents that are best placed to assist the GCSB in relation to a matter under Part 3 of the TICSA.

When to Notify

The duty to notify or engage with the GCSB about certain proposed decisions, courses of action or changes is found in sections 48 and 46(1) of the TICSA.

It is important to **keep in mind that not all proposals require notification**. This section explains what kinds of proposals need to be notified, and when.

The TICSA framework ensures the GCSB receives, with the collaboration and input of network operators, the information needed to properly consider, and make decisions about network security risks.

The GCSB will follow the same process to identify and address network security risks for proposals notified under both sections 48 and 46(1).

Section 48 – Proposals Affecting Areas of Specified Security Interest

Section 48 of the TICSA creates the obligation for network operators to notify the GCSB of proposals (proposed decisions, courses of action or changes) in regard to certain parts of their network.

Section 48 Network operator must notify Director

(1) A network operator must notify the Director of any proposed decision, course of action, or change made by or on behalf of the network operator regarding—

  (a) the procurement or acquisition of any equipment, system, or service that falls within an area of specified security interest; or

  (b) any change—

    (i) to the architecture of any equipment, system, or service that falls within an area of specified security interest; or

    (ii) that may affect the ownership, control, oversight, or supervision of any equipment, system, or service that falls within an area of specified security interest.

(2) The network operator must—

  (a) comply with subsection (1)(a) before any steps are taken, as part of the procurement or acquisition decision-making process, to approach the market (whether by request for quote, tender , or otherwise) or comply with subsection (1)(b) during the development of a business or change proposal; and

  (b) ensure any notice given to the Director in compliance with subsection (1) is given within sufficient time for the Director to consider whether to take action under section 51.

"*Proposed* decision, course of action, or change..."

The timing of notification is important. Network Operators are required to notify the GCSB at the stage when the decisions, courses of action or changes described are still proposals, yet to be implemented.

If a network operator is looking at procurement or acquisitions, TICSA requires they must notify the GCSB before taking any steps, as part of the procurement or acquisition decision-making process, to approach the market (whether by request for quote, tender , or otherwise).

This means, for example, that notification is required either prior to (or at the time) a Request for Proposals (RFP) is issued. If a network operator does not use a RFP process or similar, notification is required before making the decision about procurement.

Providing notification before issuing a Request for Information (RFI) from vendors may in many cases be too early, however some network operators may choose to provide notification at this point if the scope of the proposal is narrowed so it can be practically assessed.

With any other change to the network in an area of specified security interest, network operators are required to notify the GCSB during the development of a business or change proposal.

These requirements are to ensure the GCSB has sufficient time to consider proposals and take action if needed. They also enable any network security risks to be identified and addressed as early as possible in the network operator's procurement or change process. Allowing sufficient time for the GCSB to consider proposals will also help ensure minimal disruption to network operators' plans.

"... decision, course of action or change"

A proposed decision, course of action or change includes standard builds which might cover a particular change replicated at many points of a network, and also 'bulk changes' – a series of changes that can be treated as one overarching 'bulk change'.

Network operators can submit a single (rather than repeated) notification for a standard build or a bulk change.

Standard builds

A standard build may be a consistently procured equipment build or network addition, which is replicated throughout the network. Notification of the standard build is only required in the first instance, provided the build does not change to a type of equipment that has not been previously submitted by that network operator. In instances where a standard build is used, notification should also include details of the geographic locations in which it is intended to be deployed.

An example of a standard build would be a build which is replicated across the country. In such a case, a notification of proposal which specifies which equipment will be used, the oversight and control mechanisms and the geographic locations that the build will be deployed in would be sufficient notification for all deployments of the same build (provided no network security risks are identified).

Should the standard build change from that notified to the GCSB, a new notification would need to be submitted, that outlines what is changing in the new build.

Bulk changes

In addition, one notification may be submitted for a standard set of equipment to be used in a network proposal, i.e. a bulk change. This could include all versions of a certain type of networking equipment, and the software/firmware builds that are likely to be deployed on it.

Notification could also be supplied for a specific product range which may change incremental versions over time. Once the GCSB has considered the proposal covering the product range, the equipment would be able to be deployed on the network without the need to submit a new notification.

> *One example of a bulk change would be a notification of proposal which outlines a product range of network cards which would be deployed in a network switch. Once assessed, provided no network security risks were identified, the equipment would be able to be deployed without needing a new notification (such as a capacity upgrade).*

However there are some practical limitations to notifications of bulk changes. A notification with an excessive number of equipment types or for an entire vendor's product range does not amount to notification of a bulk change.

"Areas of Specified Security Interest"

Only proposed decisions, courses of action or changes that affect an "area of specified security interest" need to be notified under section 48.

Section 47 of the TICSA defines term:

(1) In this section and section 48, an area of specified security interest, in relation to a network operator, means—
- (a) network operations centres:
- (b) lawful interception equipment or operations:
- (c) any part of a public telecommunications network that manages or stores—
  - (i) aggregated information about a significant number of customers:
  - (ii) aggregated authentication credentials of a significant number of customers:
  - (iii) administrative (privileged user) authentication credentials:
- (d) any place in a public telecommunications network where data belonging to a customer or end user aggregates in large volumes, being either data in transit or stored data:
- (e) any area prescribed under subsection (2).

Although many of these terms are common to network operators, some further guidance on what they mean is provided below.

a) **Network Operations Centres** (NOC) – The NOC is the function or functions through which network operations are controlled, either as a function distributed among business units, or as a discrete business unit in itself.

   This includes Security Operations Centres (SOCs) if distinct from the NOC (since they also perform key functions of network governance and oversight). Proposals that affect the operation of the NOC or SOC, their oversight, control, and effective supervision, as well as core equipment used must be notified.

b) **Lawful interception equipment or operations** – Any equipment designed to facilitate the lawful interception of communications on a network, which is permanently installed on the network, or able to be installed on request. For the purposes of this guidance, this also includes hardware or software which supports or facilitates this function.

c) **Parts of networks that manage or store aggregates of information** – These are the places where sensitive information is likely to be stored, making the systems hardware and its support/operation of specific security interest.

   i. *Aggregated information about a significant number of customers*. This refers to:
      - Databases which store data in bulk, such as call records or network traffic data.
      - Operations Support Systems (OSS), or Business Support Systems (BSS) and other forms of business customer databases.
      - Proposals affecting the equipment or systems which interact directly and modify the network core require notification.

   ii. *Aggregated authentication credentials of a significant number of customers*. This refers to:
      - Areas of the network which store authentication credentials & encryption keys.
      - The Evolved Packet Core (EPC) and the Home Location Register (HLR/HSS) in mobile networks.

   iii. *Administrative (privileged user) authentication credentials*. This refers to:
      - Places where privileged user credentials are stored and audit and oversight controls are retained.

d) **Places where data belonging to customers or end users, aggregates in large volumes, either in transit or at rest**. – In particular, this covers:

   i. Large databases which reside in the core of the network and customer Voice Mail Systems (VMS), large email or message systems; and

   ii. Points of interconnection or intersection with other networks, and other areas over which a significant proportion of the traffic on the network travels, in each case where the volume of traffic is, in absolute terms, 15% or greater of the total traffic travelling over the network.

Changes made prior to 11 May 2014

Network operators do not need to notify GCSB of decisions, courses of action or changes which were initiated prior to the TICSA coming into effect on 11 May 2014.

If a decision, course of action or change is not implemented before 11 May, and after 11 May is changed substantively (such as the re-issuing of an RFP), the decision, course of action or change falls within section 48, the network operator must notify the GCSB.

Section 46(1) – Identified Potential Network Security Risks

A network operator must engage with the GCSB as soon as practicable after becoming aware of any network security risk that may arise if the proposed decision, course of action, or change is implemented.

If a network operator becomes aware that by implementing a proposed decision, course of action or change – to any part of their network – a network security risk may arise, they are required to engage with the GCSB.

In some cases a known security risk may be identified in a network by a network operator. A network operator can look to the factors listed in section 50 of the TICSA to help identify if an implemented decision, course of action, or change might give rise to a "network security risk".

To keep the network security processes streamlined, network operators will need to notify the GCSB of the possible network security risk using the notification template supplied. For ease of consideration these will be treated in the same way as a section 48 notification.

Exemptions from Duty to Provide Notification

Exemptions from the duty to notify can be granted by the Director of the GCSB, but only if satisfied that the granting of an exemption will not give rise to a network security risk (section 49).

Exemptions can be granted to individual network operators or a class of network operators. The GCSB will notify individual network operators directly in writing of any exemption applying only to them. Exemptions that apply to a class of network operators will be published on the GCSB website. Written notification will also be sent to all network operators falling in that class.

Network operators will be able to request exemptions from the GCSB using a template that will be supplied. They will need to provide enough information to allow consideration of whether granting the exemption would give rise to a network security risk or not.

Exemptions have to be set out in a separate notice issued by the Director. When the TICSA comes into force, any exemptions the Director decides to grant as a result of the consultation process around this document will be notified to network operators.

The following proposals do not need to be notified because they fall outside the TICSA's notification requirement.

- Proposals initiated prior to the network security provisions of the TICSA coming into force (11 May 2014)
- Changes to areas of networks outside section 47 (Areas of Specified Security Interest), unless the changes may give rise to a network security risk (section 46 (1)).
- Any area/change outside of the network operator's control.

The following exemptions are currently under consideration. If they are granted, the Director will issue an emption notice. The exemptions would come into effect at the same time as the TICSA, on 11 May 2014.

Please note these areas are not exempt until a Director's exemption notice is issued.

Proposed Exemptions

This Guidance paper proposes that **notification will *not be required* for the following**:

- Any change to a network which is a part of the maintenance, support, and day to day running of a network to ensure its availability

  This includes:

  - *patching, software or firmware version updates,*
  - *changes which do not alter the architecture or configuration of the network,*
  - *changes to equipment, systems or services which supply infrastructure support (including power, air conditioning & fire suppression systems),*
  - *equipment, systems or services used in generic office management (such as office supplies, printers, fax machines, desktop computers or thin clients, screens),*
  - *changes to routing within the network.*

  The exemption does not include a change to a network which is a part of the maintenance, support and day to day running of a network to ensure its availability that has been specifically identified as a change that could give rise to a network security risk during GCSB's consideration of an earlier proposal.

- Changes in configuration or layout of any network equipment, system or service provided they do not impair the network operators effective ownership, control, oversight, or supervision of any equipment, system, or service (inconsequential changes).
- Changes to augment or optimise existing network, systems or services with equipment, systems or services of the same make, model or type.
- Updates to fix bugs, and replacements necessary to resolve faults in any network equipment, system or service.
- Any change to equipment, systems or services which has previously been notified to the GCSB and no network security risk was identified, provided the change to the equipment, system or service does not materially differ from the proposal previously considered, and provided the change does not affect the ownership, control, oversight, or supervision of any equipment, system, or service.

  This covers for example, the procurement or replacement of equipment that has previously been considered by GCSB under the TICSA process with no network security risk identified, provided it is the same make, model and type. If the replacement equipment is significantly different, a new proposal will need to be submitted.

- Any standard build or bulk change which has been previously notified can be replicated without the need for a new notification, provided it was considered by GCSB not to give rise to any network security risks.

  This is also provided that the build or bulk change do not change in a way that is different to what was considered. Any changes to what was notified as a standard build or bulk change need to be notified to the GCSB as a new proposal.
- Any testing, experimentation or trials on equipment connected to the network that started before the network security provisions of the TICSA came into force, or any testing, experimentation or trials on equipment that is not connected to the public telecommunications network.

  For example, this would cover testing conducted in a staging environment prior to being deployed on a production environment, provided suitable controls have been employed to isolate their test environment from their production network.

- Any decision, course of action or change that is the implementation of the results of a test, experiment or trial that was previously notified to the GCSB and:
  - No network security risk was identified by the GCSB; or
  - The network operator provided a mitigation plan that was accepted by the GCSB as preventing or sufficiently mitigating the identified network security risk.

- Any replacement of existing equipment, systems or services already installed on a network before the network security provisions of the TICSA came into force, with equipment, services or systems of the same make, and similar model.

  A "similar model" includes standard upgrades, or logical version replacements. If the replacement equipment, systems or services are of a different make, notification of a proposal will need to be submitted.

- Replacements of existing network equipment, systems or services of the same make, or model, including standard upgrades, or logical version replacements (such as in-line replacements for equipment at the end of its supported life, or equipment which is of the same type but has greater capacity to perform the same function i.e. capacity upgrades).
- Any accelerated business change process (emergency changes) that requires deployment of a solution to maintain the availability of a network, or any service or product that operates on that network before notification can reasonably be given, provided that the network operator notifies the GCSB as soon as practicable after the change is made.
- Any customer premise equipment (CPE) deployed onto a private network that is not owned, operated or controlled by the network operator, provided it is not configured to modify or control the core network of the operator in a way which could affect the ownership, control, oversight, or supervision of any equipment, system, or service.

  This includes for example home routers, or servers and databases sold to a business customer, provided the operator's network is configured to limit the customers' ability to modify the core of the network.

If in Doubt...

Especially at the start of the TICSA process, network operators may be unsure whether a specific proposal needs to be notified or not. Network operators can contact the GCSB for general guidance about the scope of the notification requirements, but for the avoidance of doubt, network operators should notify the GCSB of the proposal through the template notification form.

If the GCSB receives a notification of a proposal that does not in fact fall within the TICSA requirements, network operators will be contacted as soon as possible to let them know the notification is not required.

Form of Notification

A standard template has been created for all network operators to notify the GCSB of proposals. The GCSB will only accept notifications made using this template. This will assist in the speed of consideration by ensuring a consistent approach by all network operators and that all necessary information is provided up front.

Notification will not be considered to have been made, until all relevant and necessary information has been provided by the network operator to the GCSB.

The Notification template will be made available on the GCSB website before 11 May 2014. Notifications can then be submitted in hard copy or by email. In order to ensure the GCSB is able to consider whether the proposal gives rise to a network security risk, the following information will be required on the template;

- Nature of the proposal, objectives, what it is replacing or if it is a new system, the service or function, and an outline of the design and security considerations (self-identified).
- Hardware, software, vendors, services used and any subcontractors expected to be involved in or considered under the proposal (if known).
- Which section the notification is made under:
  - section 48 (proposed decisions, courses of action or changes affecting areas of specified security interest) or,
  - section 46(1) (network operator has identified a potential network security risk regarding any part of their network).

- Timeframes the network operator is working to (such as proposed dates of RFP or similar process, decision making timeframes).
- Any identified security risks in the proposal.
- Any additional information relevant to assess the proposal, (this can include material taken from business cases, security/risk assessments; details of any applicable standards used, and network architecture diagrams).
- When providing notification about a change to Services, network operators will need to provide sufficient information to understand the service that will be provided, how the effective ownership, oversight and control is exercised and the security controls that will be employed.
- Points of contact for further information including;
  - Full Name
  - Position Title
  - Contact Phone Numbers
  - Email Address
  - Physical Address
  - Clearance Status (if known)

After submitting their notification of a proposal to the GCSB, network operators can continue with the planning phase of their project while their proposal is considered.

Section 3:
How does it Work?
A Step By Step Guide

The Network Proposal Process

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

The process is *illustrated in the 'Network Proposal Process' (Figure 1)* on page 17

The Process

1. If a network operator is considering a proposed decision, course of action or change in relation to its network (i.e. a proposal) the network operator must consider whether it has to be notified to the GCSB:
    - If it affects an area of specified security interest (section 48), or
    - The network operator believes it gives rise to a potential network security risk (section 46(1)),
    - And is not covered by an exemption (section 49).

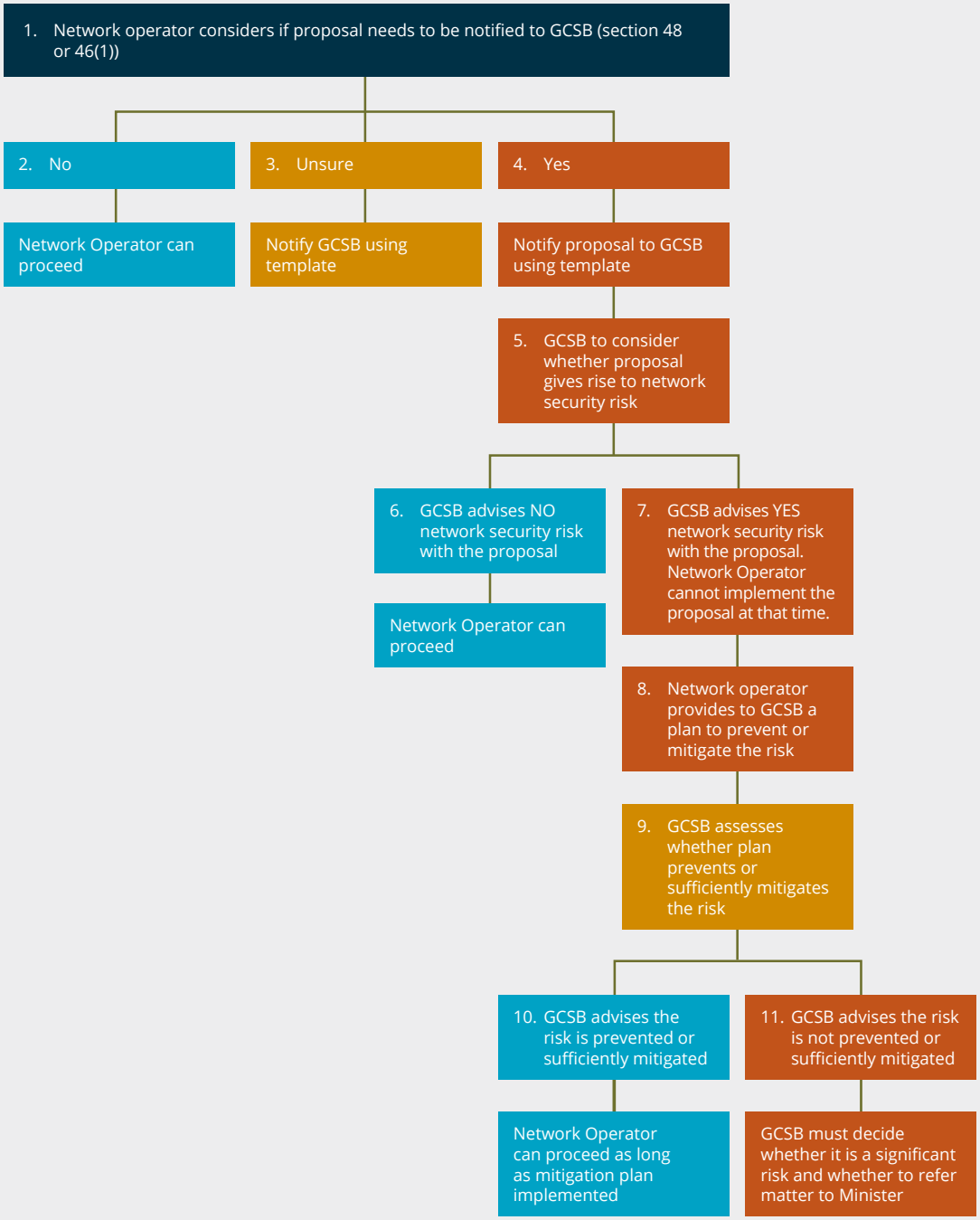
2. If the proposal **does not** affect an area of specified security interest, or is covered by an exemption, then no notification is required and the Network Operator can **proceed with the proposal**.
3. If it is **unclear** whether a proposal falls within the notification requirements of sections 48 or 46(1), or is covered by an exemption, for the avoidance of doubt, Network Operators should **notify the GCSB**.
4. If the proposal **does fall within the notification requirements**, then details of the proposal, containing all of the information outlined in this Guidance, and the template, **must be supplied to the GCSB**.
5. The GCSB will **consider whether the proposal gives rise to a network** security risk In doing so, the GCSB must consider the factors outlined in section 50(1)(a), (b) and (c) of the TICSA.
6. If the GCSB considers the proposal **does not give rise to a network security risk** Network Operators will be advised in writing and they **may proceed with the proposal**.
7. If the GCSB considers the proposal **does give rise to 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)).
    - 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.

8. After being advised that a proposal raises 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)). Mitigation may include withdrawing a proposal.
9. The GCSB will assess **whether the plan prevents or sufficiently mitigates the risk** (to the point that no, or minimal, network security risk remains) and will notify the network operator of the outcome in writing.
10. If the GCSB considers 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 52(3)(b)).
11. If the network operator's mitigation plan does not prevent or sufficiently mitigate the network security risk, and that risk is a significant network security risk, **the Director of the GCSB can decide to refer the matter to the Minister for the GCSB** who can issue a direction requiring the network operator to carry out certain actions to mitigate or prevent the risk. This process is explained later in this Guidance.
12. If the Director 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.

Further detail:

The GCSB can require network operators to provide information (section 78 of the TICSA). If further information is requested under section 78, the Network Operator must provide it within the timeframe requested, or if not specified, within 20 working days (section 79).

Figure 1: The Network Proposal Process



Note: A proposal may be withdrawn at any time by supplying notification in writing to the GCSB.

Section 4:
Understanding Risks

Consideration of Network Security Risk

Section 50 of the TICSA requires the GCSB to consider whether a proposed decision, course of action or change to an area of specified security interest in a network gives rise to a network security risk, or a significant network security risk.

> Section 50 (1) When considering whether a network security risk or significant network security risk is raised under this Part, the Director, or if the case requires, the Minister responsible for the Government Communications Security Bureau,—
>
> (a) must consider the likelihood that the matter giving rise to the risk will lead to—
>
> (i) the compromising or degrading of the public telecommunications network; and
>
> (ii) the impairment of the confidentiality, availability, or integrity of telecommunications across the network; and
>
> (b) must consider the potential effect that an event described in paragraph (a)(i) or (ii) will have on the provision of—
>
> (i) central or local government services:
>
> (ii) services within the finance sector:
>
> (iii) services within the energy sector:
>
> (iv) services within the food sector:
>
> (v) communication services:
>
> (vi) transport services:
>
> (vii) health services:
>
> (viii) education services; and
>
> (c) may consider any other matter that the Director or Minister considers relevant.

GCSB's consideration of network security risk involves consideration of the likelihood that the proposal (or part of it) will lead to the compromise or degradation of the public telecommunications network, and the impairment of the confidentiality, availability or integrity of telecommunications across the network, and the potential effect of that on the provision of important services.

As explained earlier in this Guidance, consideration will not be given to 'general' network security risks (that is, network security risks which do not intersect with national security). A consistent methodology will be used to consider all proposals against the factors identified above.

> *An example of a possible network security risk would be if a network operator's proposal included allowing remote access to a core part of their network management system. This would be based on, in part, an assessment that controls are insufficient and could allow a motivated attacker to disable or compromise the network.*
>
> *Included in this assessment would be consideration of the likelihood of a successful compromise occurring and the impact that a successful attack would have on key services which were critically dependent on that network.*

The GCSB will draw on a range of information, including:

i. the nature of the equipment
ii. the operational model;
iii. the network area;

iv. whether independent assurance can be provided, for example, compliance with international standards, opportunity for an independent software audit;

v. information about any of the companies involved, including past behaviour, any examples from other jurisdictions; and

vi. classified information uniquely available to GCSB.

This list is not exhaustive, and the relative weight of each factor may vary from proposal to proposal.

The GCSB will endeavour to provide network operators with unclassified information to assist in their understanding of a network security risk. Where possible GCSB will also share further information about identified network security risks and about controls or mitigations with the security cleared representatives of the network operator, to assist them in providing informed guidance to their organisation.

The GCSB will also assist the security cleared representatives to identify information that can be shared further within the business.

Assessment of a Plan to Prevent or Sufficiently Mitigate a Network Security Risk

The GCSB must assess whether the proposed prevention or mitigation plan will, if implemented, prevent or sufficiently mitigate the network security risk(s) that were identified. Mitigation or prevention plans could include;

- Compensatory controls & plans to manage the risk over time
- Preventative measures to avoid the risk
- Withdrawal of the part of the proposal which creates the risk
- Inclusion of security clauses in commercial contracts

Included in this assessment will be consideration of whether the plan removes or prevents the network security risk, or whether compensatory controls can sufficiently reduce the network security risk to an acceptable level (no, or minimal network security risk).

> *Using the example supplied previously, an example of a prevention plan could be to remove the remote access element of the proposal altogether, given the sensitivity of the access it would allow.*
>
> *Alternatively, a mitigation plan may include controls such as additional logging, multi-factor authentication and restricting access to other parts of the core when using remote access.*

When communicating decisions about network security risks, the GCSB will provide what information it can in order to identify the areas of concern within a proposal, so network operators can develop a better understanding of the network security risks as understood by the GCSB.

> *Another example could be a proposal to build a new core service platform for business customers. The GCSB may consider a network security risk the fact that known vulnerabilities exist in the firmware of the equipment which could result in the wide scale leak of authentication credentials.*
>
> *The mitigation plan proposed by the network operator could involve increased controls around authentication for the service, and follow up notification to the GCSB once the vulnerability was patched in a later version.*

Communication of Outcomes

At each stage of the process, the GCSB will notify the network operator of the GCSB's conclusion about network security risk.

At the completion of an initial consideration, written notification will be issued that a proposal either;

a) **does not give rise to a network security risk** and the network operator may continue with the proposal, or;

b) **does give rise to a network security risk** and the network operator cannot implement the proposal at that time (section 51(1)(b)) and is required to provide a mitigation plan as soon as practicable (section 51(3)).

After assessing a network operator's prevention or mitigation plan, the GCSB will advise the network operator in writing that either:

a) the proposed plan (or parts of it) to prevent or mitigate the risk has been accepted, and the network operator may proceed to implement the proposal as modified by the mitigation plan; or,

b) the proposed plan to prevent or mitigate the risk has not been accepted because it does not prevent or sufficiently mitigate a significant network security risk identified.

The GCSB will advise the network operator whether the Director has decided to refer the case to the Minister or not.

Summary of Timeframes

Minimising disruption to Network Operator's decision making processes is a fundamental part of the approach incorporated in the TICSA and this Guidance. Under section 8(2) the GCSB is subject to the principle that steps taken by the GCSB should be made or taken as soon as practicable.

Therefore, while no deadlines are imposed by the TICSA, this section gives an indication of the timeframes anticipated during the proposal consideration process.

The GCSB will provide a decision to the notification of proposal to the network operator as quickly as possible. Where a proposal is received that either does not require notification or an assessment can be completed quickly the GCSB will aim to respond to network operators as soon as possible, and within the time frames noted below.

Initial Notification:

In all cases the GCSB will acknowledge receipt of a notification from a network operator once *all* of the information described in the Form of Notification section has been provided, this will be no more than three working days.

Written notice of the outcome of the GCSB's consideration of the notified proposal will be given within 20 working days of the date of acknowledged receipt of the notification. If an extension of time is anticipated, the GCSB will contact the Network Operator to discuss as early as practicable, followed by confirmation in writing prior to the end of the 20 working day limit.

It is important that the GCSB receives full and complete information on the proposal. If additional information is required the GCSB will contact the network operator to request this information. The 20 working day period for consideration of network security risk cannot begin until all requested information is received. If the assessment requires less than 20 days to complete, the outcome will be notified as soon as practicable.

After Notification of a Network Security Risk

In the event that a network security risk is identified, the network operator is required to provide its prevention or mitigation plan to the GCSB as soon as practicable.

Once the prevention or mitigation plan has been provided, along with any additional information relevant to it, the GCSB will acknowledge receipt of the plan; this will be within three working days.

The GCSB will assess the mitigation plan, and if it prevents or sufficiently mitigates the identified network security risks, will inform the network operator of this in writing.

If the Director intends, or is considering referring the proposal to the Minister, the Director is immediately required to seek a view by the Commissioner of Security Warrants.

These situations are likely to require an extension on the 20 working day timeframe. In these cases the GCSB will contact the network operator to discuss and confirm in writing prior to the end of the 20 working day limit.

Section 5:
Referrals

Referral to the Minister

To ensure significant network security risks are addressed, the TICSA includes provision for the Minister of the GCSB to make a direction requiring a network operator to take steps to prevent, sufficiently mitigate, or remove the network security risk (section 57).

The Minister can only make a direction if a case has been referred to him or her by the Director of the GCSB. The Director can only refer a case to the Minister if there is a significant network security risk that has not been addressed, or if a network operator does not comply with certain duties (the duties are set out below).

The Director can refer a case to the Minister if –

- a mitigation plan does not prevent or sufficiently mitigate a significant network security risk; or
- a network operator, despite being advised by the GCSB that a proposal cannot be implemented (s51), enters into a binding legal arrangement, implements a decision or commences a course of action or change that gives rise to a significant network security risk; or
- a network operator fails to comply with a requirement to provide information to the GCSB (s78) and has entered into a binding legal arrangement, implemented a decision, or commenced a course of action or change that gives rise to a significant network security risk.

If the Director is considering referring the case they must seek the view of the Commissioner of Security Warrants about the network security risk that has been identified (section 56).

If the Director does decide to refer the case to the Minister, the network operator will be notified and will be invited to make submissions to the Minister.

The Minister has to base their decision to issue a direction on a series of factors – these include those the Director must consider in identifying network security risk (section 50) and also those set out in section 57(2) of the TICSA:

(2) Before making a direction under this section, the Minister must –

(a) have regard to –

(i) the nature and extent of the network security risk

(ii) the impact on the network operator of meeting costs associated with the direction

(iii) the potential consequences that the direction may have on competition and innovation in telecommunications markets

(iv) the anticipated benefits to New Zealand from preventing, sufficiently mitigating, or removing the network security risk

(v) the principle in section 8(4)[which is – The principle that the decision or exercise of the function or power should be proportionate to the network security risk.]

(vi) the potential impact of the direction on trade

(vii) any other matters that the Minister considers relevant; and

(b) be satisfied that the direction is consistent with the purpose in section 7. [note reference in Guidance already]

The Minister must also consult with the Minister of Trade and the Minister for Communications and Information Technology, and he or she must be satisfied that exercising his/her powers is necessary to prevent, sufficiently mitigate, or remove a significant network security risk.

A Ministerial direction will be issued in writing to the affected network operator, with reasons (not including those parts of the reasons that would reveal classified information).

Non-compliance with a Ministerial direction is considered a serious non-compliance under the TICSA and could result in an enforcement notice issued against the network operator by the Director of the GCSB, or a compliance pecuniary penalty order from the High Court.

Guidance Revisions

This Guidance may be amended from time to time for various reasons including if there are any changes to the notification requirements, or to the process for notification.

In the event that major revisions of the guidance are necessary, the GCSB will consult with network operators as part of the revision process. Major revisions are considered to be any changes which substantively change one or more sections of the Guidance.

In the event that minor revisions are required, consultation may not be initiated. Minor revisions are considered to be any changes which do not substantively change one or more sections of the Guidance.

Each revision of the guidance will be supplied to the designated point of contact for a network operator, as provided in their registration details under Part 4, Section 62 of the TICSA.