GOVERNMENT COMMUNICATIONS SECURITY BUREAU

TE TIRA TIAKI

Telecommunications (Interception Capability and Security) Act 2013

Guidelines for Network Operators

Publication Date: 27 May 2020

www.ncsc.govt.nz

www.gcsb.govt.nz

New Zealand Government

Contents

TICSA Guidelines

The following Guidance has been prepared to support the 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.

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 TICSA only apply to network operators as defined in that Act.

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 proposed 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.

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-General 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-General 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-General of the GCSB under section 58 of the TICSA, to provide information about the requirements on network operators under Part 3 of the TICSA.

The Guidance is subordinate to 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 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 proceedings related to TICSA, compliance with the Guidance will be treated as evidence of compliance with the applicable requirements in the legislation (section 58).

TICSA places network security regulation responsibilities on the Director-General of the GCSB and so refers to "the Director-General" 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-General 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.

Please raise any questions you have about the processes and responsibilities laid out in the Guidance 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 inferred from the list of factors in s 50 that the GCSB must consider when deciding whether a network security risk or significant network security risk is raised.

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; and
    - the impairment of the confidentiality, availability or integrity of telecommunications across the network; and,
- the potential effect of that on the provision of certain services (including for example, central or local government services, health or transport services); and
- Any other matter that the GCSB considers relevant.

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

The focus on New Zealand's national security in the Part 3 TICSA 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 for the purpose of Part 3 TICSA, 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.

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 three 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. [1]

[1]http://www.police.govt.nz/advice-services/businesses-and-organisations/telecommunications-interception-capability-security-0

Section 1 – 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-General in relation to any matter in this Part [Part 3 of TICSA].

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. For example, a network operator engaging with 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).

Application of Part 3 of TICSA to smaller network operators

Under Part 3, all network operators, regardless of size, must notify the GCSB under s 48 of the Act of any proposed decision, course of action, or change within a specified area of security interest.

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-General

(1) A network operator must notify the Director-General 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-General in compliance with subsection (1) is given within sufficient time for the Director-General 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 of any equipment, system, or service that falls within an area of specified security interest, 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. This would include for example notifying of purchasing of or sale to, another organisation, changing a contracted third party provider, and changing remote access methods and/or authentication.

These requirements are to ensure the GCSB has sufficient time to consider proposals and fulfil its regulatory function under TICSA. They also enable any network security risks to be identified and addressed as early as possible in the network operator's decision, course of action, 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.

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 area of specified security interest:

(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 – Are any equipment used to provide Lawful Intercept solutions as part of Section 2 of TICSA

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 and 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:

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

v. Any part of the network through which a significant proportion of the traffic on the network travels. This includes points of interconnection or intersection with other networks or aggregation points within the network. i.e. at the point of interconnection where the traffic of 10000 or more end-users may be impacted.

Section 46(1) – Network operator identified 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 may notify the GCSB of the network security risk using the notification template supplied. These will be treated in the same way as a section 48 notification.

Exemptions from Duty to Provide Notification

Exemptions from the duty to engage and notify pursuant to ss 46(1) and 48, may be granted by the Director-General of the GCSB, if the Director-General is satisfied that the matter to which the exemption relates 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 may request exemptions from the GCSB. A template for such requests is available on our website. Sufficient information is required to allow consideration of whether the matter to which the requested exemption relates will give rise to a network security risk or not.

Exemptions are set out in a separate notice issued by the Director-General.

The current exemptions applicable to all or a class of network operators are available on the NCSC website: www.ncsc.govt.nz/ticsa

If in Doubt…

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 is not required to be notified under TICSA, 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.[2] This will assist in the speed of consideration by ensuring a consistent approach by all network operators and that necessary information is provided up front.

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

The Notification template is available on the GCSB website. Notifications can 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, as a start point the following information will be required;

- 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.

[2] http://www.ncsc.govt.nz/ticsa