National Cyber Security Centre

Regulatory Strategy

For network security under Part 3 of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA)

Te Tira Tiaki
Government Communications Security Bureau

www.ncsc.govt.nz

Contents

Ngā kaupapa

This Regulatory Strategy outlines how the NCSC exercises powers and functions under TICSA on behalf of the Director-General of the GCSB, and the NCSC's general approach to regulation.

Terms used in this strategy

Compliance

'Compliance' refers to network operators complying with their legal obligations as regulated entities under part 3 of TICSA, e.g. the requirement to notify certain proposed changes to networks under section 48.

Compliance activities

'Compliance activities' comprises all activities the NCSC undertakes as a regulator (our regulatory toolkit) with the intention of lifting network operator compliance. It includes education, guidance, early resolution and pre-enforcement actions such as warnings, as well as enforcement.

Enforcement

'Enforcement' is a type of compliance activity and specifically refers to the enforcement powers we have under TICSA.

Disclaimer: This strategy document sets out the regulatory goals, functions and responsibilities of the National Cyber Security Centre's Regulatory Unit. It is not intended as guidance issued under section 58 of TICSA and cannot be taken as evidence of compliance with the applicable requirements in the legislation.

The Regulatory Unit can be contacted by email at: **ticsa@ncsc.govt.nz**. We encourage you to contact us if you require assistance or advice.

Section 1. Our vision, purpose and outcomes

The Director-General of the GCSB has a regulatory role for the security of New Zealand's public telecommunications networks. This strategy outlines how the NCSC carries out its regulatory functions to help keep public telecommunications networks secure.

Our vision – what we want to achieve

Network security risks to New Zealand's public telecommunications networks are minimised, strengthening New Zealand's national security.

Our purpose – what drives our work

Supporting network operators to become aware of potential security risks in their networks, and to prevent or mitigate these from eventuating.

Our intended outcomes

1. Registered network operators are well-informed and aware of their obligations.
2. Registered network operators comply with their obligations.
3. Potential more-than-minimal network security risks are identified and addressed.

Section 2. Our regulatory role

Who we are

The National Cyber Security Centre (NCSC) is part of the Government Communications Security Bureau (GCSB). The NCSC's central vision is a New Zealand where good cyber security happens everywhere, all the time, by everyone.

The Regulatory Unit is located within the NCSC and is the team responsible for the day-to-day network security regulatory functions under TICSA on behalf of the Director-General.

We assess proposed changes to networks notified by network operators under TICSA to identify any potential network security risks. Our role includes working with network operators to identify and address network security risks that may arise in the process of designing, building, or operating public telecommunications networks, and to collaborate and co-operate in the prevention or sufficient mitigation of these risks.[1]

[1]Please refer to our guidelines on the NCSC website for detailed information on how to comply with the legislative requirements.

Our guiding legislation

The purpose of TICSA is:

- Interception capability: ensuring that surveillance agencies can carry out lawful interception of telecommunications (New Zealand Police is responsible for this under Part 2 and maintains the register of network operators).
- Network security: preventing, sufficiently mitigating or removing security risks from public telecommunications networks (we are responsible for this under Part 3).

TICSA empowers the Director-General of the GCSB to:

- issue exemptions to the notification requirement under section 49
- consider notifications submitted by network operators about their operation and design of public telecommunications networks for potential risks under section 50
- refer matters of network security risks to the Minister under section 54
- provide guidelines on TICSA requirements under section 58
- require information under section 78
- undertake enforcement under sections 88, 90, and 91.

As an effective regulator our aim is to use the full set of tools at our disposal to encourage compliance with the statutory framework to prevent, sufficiently mitigate, or remove network security risks.

How does TICSA work?

Part 3 requirements under TICSA apply to any person who falls within the definition of a network operator. A network operator is a person who:

- owns, controls, or operates a public telecommunications network; or
- supplies (whether by wholesale or retail) another person with the capability to provide a telecommunications service.

Network operators must notify GCSB's NCSC if they want to make certain changes to their networks that may intersect with national security (section 48). Network operators must engage with us as soon as practicable after identifying a network security risk that may arise if a change is made and must act honestly and in good faith.

GCSB and network operators have obligations under TICSA. That includes how we work together.

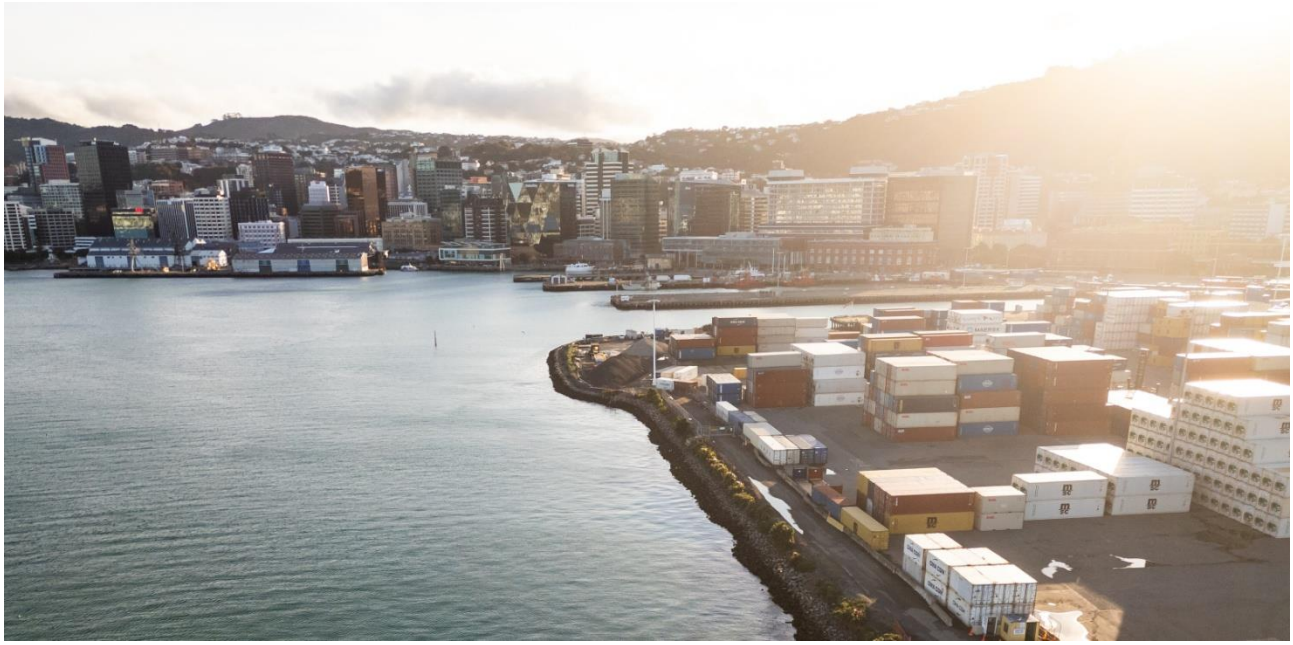
Under section 8 of TICSA, the Director-General of the GCSB and network operators must, as far as practicable:

- identify network security risks as early as possible; and
- work co-operatively and collaboratively with each other in relation to identifying and addressing network security risks that may arise.

Who we work with

We work with the Ministry of Business, Innovation and Employment (MBIE) as the administering agency of TICSA on regulatory stewardship and ensuring legislative settings remain fit for purpose.

We also work with New Zealand Police who maintain the register of network operators and carry out some of the functions under Part 2 of the Act.



Section 3. Broad principles that guide our regulatory work

Our principles

These principles underpin our approach to regulation:

Transparent

We will be as open as possible about how and when we intend to exercise our regulatory powers, upholding natural justice principles. This means we will proactively signal changes in our approach and our regulatory priorities, and ensure our actions link to the outcomes we are trying to achieve.

Timely and proactive

We will act in a timely manner to make decisions and take steps as soon as practicable. We maintain self-imposed Service Level Agreement (SLA) timeframes for assessing proposals and will inform network operators where we are not able to meet these. We will take prompt action to address non-compliance.

Fair and reasonable

We will exercise our discretion responsibly and operate in a neutral and impartial manner, to make appropriate decisions which are justifiable and informed by evidence.

Co-operative and collaborative

We will engage with network operators in good faith when supporting compliance, fostering relationships of mutual trust and respect. Where we have concerns about compliance we will reach out to talk through the issues prior to taking more formal steps.

Proportionate

We use a range of graduated regulatory tools and processes matching our actions to the risk and scale of the issue, ensuring we do not place undue burdens on operators, while taking the necessary actions to address non-compliance.

Section 4. Our approach as a regulator

Our goal is to make compliance easy and achieve high levels of voluntary compliance. We do this through:

- Providing easily accessible, timely and clear information, so that network operators are aware of their obligations.
- Being proactive and approachable, undertaking outreach activities, sector engagement and welcoming discussions with network operators.

We also monitor compliance to identify, deter and address non-compliance. Monitoring also helps us to identify systemic issues that may necessitate changes to our legislative settings.

Our practical approach to conducting compliance activities under this framework will be:

- **Risk-based** – we will focus on areas and issues posing the highest levels of risk.
- **Flexible and responsive** – we use the right tool at the right time based on the specific circumstances.
- **Communicative and informative** – we will make network operators aware of our expectations and the potential consequences of non-compliance.
- **Enabling** – we support and provide guidance to network operators, to make it as easy as possible to comply.

Our considerations

We will take the following considerations into account when considering our use of the regulatory tools outlined in section 5 of this strategy:

- **Public interest** – including the potential deterrent effect, when the non-compliance occurred, customer interests, public trust or confidence in, and credibility of the regulator, and whether the issue is widespread.
- **Risk posed by non-compliance** – taking into account characteristics of the network operator (e.g. significant numbers or criticality of customers) and the nature of non-compliant behaviour.
- **Conduct** – including the frequency of the non-compliance, e.g. one-off or ongoing/repeated.
- **Attitude to compliance** – the way a network operator approaches its regulatory responsibilities and interacts with us, e.g. willingness to understand what it needs to do to comply, taking steps to fulfil this, and cooperating in good faith.
- Other considerations as appropriate.

Section 5. Our regulatory toolkit

Information and guidance

We ensure network operators have easy access to information and guidance on the requirements of TICSA and how to comply by making information readily available on the NCSC website. Specifically, we publish Guidelines under section 58 to assist network operators to make notifications. Additionally, we provide forms and templates enabling network operators to easily notify and request exemptions from notification.

Engagement and education

We aim to make compliance easy and build strong trusted relationships with network operators. We are available to talk to operators about planned proposals and discuss areas of doubt, ensuring we work collaboratively to resolve concerns early. We are available to meet with network operators at their premises to facilitate open discussions.

From time to time, we hold TICSA Roadshows for network operators so that we can engage directly, provide reminders of obligations and our expectations, and share information.

We stay abreast of sector trends, emerging risks and evolving technology. This helps us to better understand the environment that network operators are working in, anticipate possible changes and identify potential concerns, and consider how our regulatory regime might apply to new technology.

Compliance and enforcement

We may undertake pre-enforcement action including by writing to network operators to resolve issues or concerns early, without proceeding to enforcement. We can require information under section 78 of TICSA if we consider it necessary or desirable for enforcing compliance.

We take a risk-based approach to enforcement. We can issue formal breach and/or enforcement notices for non-compliance under the Act. If unresolved, we will take further action against continued non-compliance which could lead to a court order.

Section 6. Where we are going

This is the first iteration of our Regulatory Strategy. This will be an evolving document, and we will periodically update this as we continue to develop our capability to achieve our regulatory outcomes.

Some of the activities we are undertaking to support easier and greater compliance under TICSA include:

- Continuing to enhance the information we provide to ensure we reach as many operators as possible, and to make it easy to comply. With many registered network operators, we recognise it is impossible to directly engage with each individually, so we continue to develop our resources to ensure they are fit for purpose, effective and drive positive behaviour change.
- Continually adapting our stakeholder engagement strategy, using data and insights on sector trends, emerging risks and evolving technology to inform who we talk to and how we engage with them. This includes seeking one-to-many engagement opportunities.
- Refining our enforcement capability and approach. We will share external guidance with network operators as it is developed.

We look forward to continuing to work collaboratively towards our vision of minimising network security risks to New Zealand's public telecommunications networks, strengthening national security.