




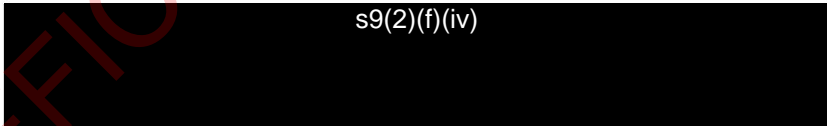
**GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU**
TE TIRA TIAKI

Briefing Paper

TICSA Notification NCSC-TN-2018-451

To Hon Andrew Little, Minister Responsible for the GCSB
From Andrew Hampton, Director-General GCSB
For your Information
Date 26 November 2018

Action sought

		Timeline
Note	I have identified a significant network security risk in regards to a notification made by Spark New Zealand Limited under s 48 of TICSA for its Phase 1 roll out of 5G services	As soon as practicable
Note	 s6(c)	As soon as practicable
Note	 s9(2)(f)(iv)	As soon as practicable
Note	In the interests of no surprises, a separate, shorter version of this briefing will be sent today to: <ul style="list-style-type: none"> • The Minister for National Security and Intelligence • The Minister of Foreign Affairs • The Minister for Trade and Export Growth • The Minister of Broadcasting, Communications and Digital Media. 	As soon as practicable

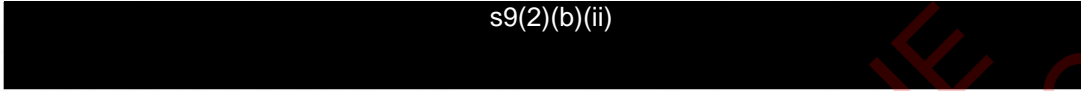
Contacts for telephone discussion (if required)

Name	Position	Telephone	1 st Contact
Andrew Hampton	Director-General, GCSB	s6(a), s9(2)	X
s6(a), s9(2)(a)	s6(a), s9(2)(a)	s6(a), s9(2)(a)	

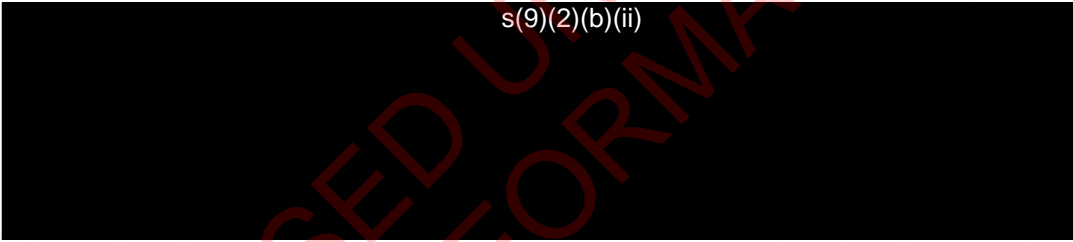
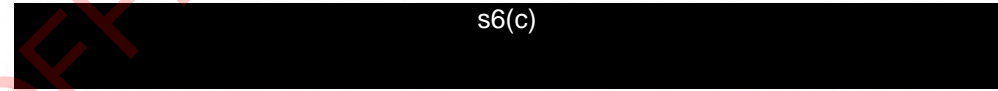
RELEASED UNDER THE OFFICIAL INFORMATION ACT

TICSA Notification NCSC-TN-2018-451

Purpose

1. The purpose of this briefing is to inform you of my decision under the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) relating to Spark New Zealand Limited's notification of its 5G Phase 1 plans.
2.  s9(2)(b)(ii)
3. The briefing also outlines the next steps in the TICSA process for this notification, including what your role as Minister Responsible for the GCSB is under TICSA.

Summary of decision

4. On 7 September 2018, Spark New Zealand Limited (Spark) notified the GCSB of its 5G Phase 1 plans under section 48 of TICSA. Further supporting information was subsequently provided, with the notification being complete on 25 October.
5.  s(9)(2)(b)(ii)
6. Part 3 of TICSA is intended to identify network security risks arising from the design, build, and operation of public telecommunications networks, and to prevent, sufficiently mitigate, or remove those risks. The Director-General of GCSB's first role is to identify whether the proposed changes would, if implemented, raise a network security risk other than a minimal network security risk, and notify the network operator.
7. In accordance with sections 50 and 51 of TICSA, I have determined that the changes proposed in Spark's notification would, if implemented, raise a **significant** network security risk.
8.  s6(c)
9. Under section 50(1)(a) of TICSA, I have considered the likelihood that the proposed change will lead to the:
 - a. compromise or degradation of the public telecommunications network; and
 - b. the impairment of the confidentiality, availability, or integrity of telecommunications across the network.

10. [Redacted] s6(a), s9(2)(b)(i)

11. In addition, I have also considered the potential effect that the compromise or degradation of the public telecommunications network, and the impairment of the confidentiality, availability, or integrity of telecommunications across the network, will have on the provision of certain services prescribed in section 50(1)(b). Those services are:
- a. central or local government services;
 - b. services within the finance sector;
 - c. services within the energy sector;
 - d. services within the food sector;
 - e. communication services;
 - f. transport services;
 - g. health services; and
 - h. education services.

12. [Redacted] s6(a)

13. [Redacted] s6(a)

Next steps

14. [Redacted] s6(a), s6(c)

15. Once notified, Spark must, as soon as practicable, respond in writing with a proposal to prevent or sufficiently mitigate the network security risk (as outlined in section 51(3) of TICSA).

16. Alternatively, Spark may choose to withdraw its notification.
17. If Spark withdraws the notification, no further action is required under TICSA. Section 48 of TICSA requires that Spark submit a new notification outlining its proposed path to 5G, which will be assessed in accordance with the Act.
18. If Spark submits a mitigation proposal, I will assess the mitigation proposal in accordance with s 52 of the Act. Under that section, I must assess whether the proposal will, if implemented, prevent or sufficiently mitigate the network security risk.
19. If I am satisfied that all or part of the proposal will, if implemented, prevent or sufficiently mitigate the network security risk, I must accept the proposal (or part of the proposal). Spark must then implement those parts of the proposal I have accepted, pursuant to s 53 of TICSA.
20. If I am not satisfied that the mitigation proposal prevents or sufficiently mitigates the network security risk, I may refer the matter to you as Minister Responsible for GCSB for a direction in accordance with processes set out in the Act.
21. Prior to referral to you, my decision must be reviewed by the Chief Commissioner of Intelligence Warrants in accordance with the Act.¹ The Chief Commissioner must be provided with all of the material (including any classified information) that informed my opinion on the network security risk. When conducting a review, the Chief Commissioner must not seek or accept any further communications from Spark. The Chief Commissioner must prepare a report and give a copy of the report to me as Director-General GCSB, as well as to Spark (subject to any redactions of those parts of the report that would reveal any classified information). I must provide you with a copy of that report if I refer the matter to you.²
22. In addition, I must notify Spark of my decision to refer a matter to you for a direction, and advise Spark that it may make submissions on the matter directly to you. I must specify a time, which must be reasonable in the circumstances, by which those submissions must be made.³
23. If I decide not to refer the matter to you, Spark may proceed with implementing the changes outlined in their notification. If I do decide to refer the matter to you, you may issue a direction in accordance with s 56 of TICSA. More about that process is set out in a section below.
24. As this is a regulatory decision-making process, there is the possibility of a judicial review at any step in the process.

¹ Refer s 56 of TICSA.

² Refer s 56(7).

³ Refer s 54(b).

Comment

25. This is the first notification the GCSB has received under TICSA that sets out a network operator's proposed path to 5G.
26. As you are aware, there has been substantial public and international interest in 5G, particularly around the role Huawei might play in 5G networks. Huawei, based in China, has become the world's largest vendor of telecommunications network equipment and services, and has been at the forefront of 5G developments.⁴

s6(a), s6(b)(i)
s6(a), s6(b)(i)

27.

s9(2)(g)(i)

28.

s9(2)(g)(i)

29.

s9(2)(g)(i)

30. GCSB has not made any public comments in relation to this notification. GCSB treats notifications under TICSA as commercial in confidence, as they often relate to design proposals which are highly commercially sensitive. We refrain from releasing the fact of, as well as any contents of, any notification. This supports open and frank disclosure.

31.

s9(2)(b)(ii)

⁴ Huawei's primary competitors are Ericsson, based in Sweden, and Alcatel-Lucent, based in France. There are a number of other major suppliers of telecommunications equipment, including Cisco, based in the United States, and ZTE, based in China.

s6(a)

Your role in the event of a referral

32. If the matter is referred to you for a direction, the matters that you must have regard to are different to the matters I am required to consider in determining the network security risk.
33. You may make a direction in accordance with s 57 of TICSA. Section 57 provides:
- (1) The Minister Responsible for the Government Communications Security Bureau may make a direction under this section only if the Minister—
 - (a) has been referred a matter under section 54 or 55; and
 - (b) has considered any submissions from the affected network operator; and
 - (c) has considered the report of the Commissioner under section 56; and
 - (d) has consulted the Minister for Communications and Information Technology and the Minister of Trade; and
 - (e) is satisfied that exercising his or her powers under this section is necessary to prevent, sufficiently mitigate, or remove a significant network security risk.
 - (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);
 - (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.
 - (3) A direction under this section—
 - (a) may require a network operator to take steps, as specified by the Minister, to prevent, sufficiently mitigate, or remove the significant network security risk, and those steps may include—
 - (i) requiring the network operator to cease a particular activity or to do or refrain from doing a particular activity in the future; or
 - (ii) directing the network operator to make changes to, or remove, any particular system, equipment, service, component, or operation on or related to the network; and

- (b) may provide for any other relevant matter.
- (4) The Minister must ensure that any time by which a network operator must comply with a requirement of the direction is specified in the direction and is reasonable in the circumstances.
- (5) The Minister must issue the direction in writing to the affected network operator together with reasons, except those parts of the reasons that would reveal classified information.
- (6) The Minister must not delegate to any person, other than another Minister, the power to make a direction under this section.

Media reporting

34. There has been extensive comment recently in the media about Huawei's role in 5G networks in New Zealand, led by comments from Spark's Mr Moutter, and Huawei NZ deputy chair Andrew Bowater. GCSB provides some factual background and context below for some of the matters raised in the media, for your awareness. The media reporting is not relevant to my decision.

s9(2)(b)(ii)

35. s6(a), s9(2)(b)(ii)

36. s6(a), s9(2)(b)(ii)

- s6(a), s9(2)(b)(ii)

- s6(a), s9(2)(b)(ii)

5 s9(2)(b)(ii)

- [REDACTED] s6(a), s9(2)(b)(ii)

37. [REDACTED] s6(a), s9(2)(b)(ii)

UK evaluation of Huawei equipment and services

38. Huawei has publicly stated that the security evaluation of Huawei products through the UK-based Huawei Cyber Security Centre (HCSEC) is evidence that Huawei's products do not present a threat to New Zealand networks.
39. HCSEC opened in November 2010 under a set of arrangements between Huawei and the UK government to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's critical national infrastructure. HCSEC employs UK security-cleared staff to provide security evaluation for a range of Huawei products used in the UK telecommunications market. The UK's National Cyber Security Centre (UK NCSC), as the national technical authority for information assurance and the lead government operational agency on cyber security, leads for the UK Government in dealing with HCSEC and with Huawei more generally on technical security matters.

40. [REDACTED] s6(a), s9(2)(f)(iv)

41. [REDACTED] s6(a), s9(2)(f)(iv)

42. [REDACTED] s6(a), s6(b)(i)

Huawei limitations on selling into the core

43. Huawei NZ has made statements to the media indicating that it is willing to forgo selling its equipment and services into the 5G network core.

44. In the 5G context, many of the sensitive functions of a network will no longer be limited to the network core, but will be distributed throughout the network, including within the RAN – the so-called network “edge”. In other words, where the “brains” of a network once resided in the core (hence why it was considered such a sensitive part of the network), those brains are now distributed throughout the network as a whole.

Huawei role in other overseas 5G deployments

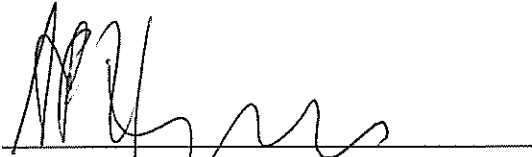
45. A number of news reports have cited Huawei’s role in providing 5G services for networks in other countries, particularly Telefonica and SK Telecom in South Korea.
46. GCSB has limited visibility to non-NZ Huawei deployments. Open Source reporting indicates a number of trials of 5G by Telefonica (which provides telecommunications services through a number of subsidiaries in Europe and other countries), though these are dated. More recently, Telefonica Argentina indicated it would be rolling out 5G using Ericsson.
47. In September, open source reporting showed that SK Telecom announced that it was seeking bids for its 5G deployment from vendors other than Huawei (including Samsung, Ericsson, and Nokia).
48. [REDACTED] s6(a), s9(2)(g)(i)

Reported pressure from US and Australia

49. There have been various media reports that the New Zealand Government has been subject to pressure from its US and Australia counterparts regarding Huawei’s involvement in 5G deployments here. While GCSB receives relevant intelligence from its US and Australian partner agencies, there has been no pressure to adopt a particular position. It is well recognised that New Zealand will make an independent decision in accordance with its legislative framework.

Talking points

50. [REDACTED] s9(2)(f)(iv)



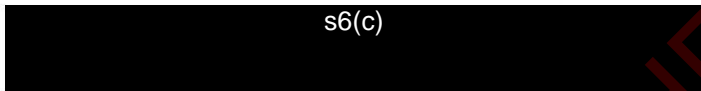
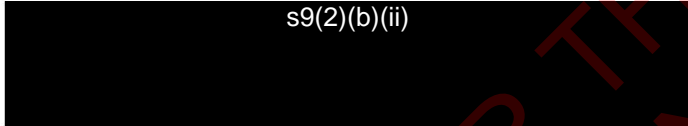
Andrew Hampton

Director-General, GCSB

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Recommendations

It is recommended that you:

1	Note	I have identified a significant network security risk in regards to a notification made by Spark New Zealand Limited under s 48 of TICSA for its Phase 1 roll out of 5G services	Yes/No
2	Note	 s6(c)	Yes/No
3	Note	 s9(2)(b)(ii)	Yes/No
4	Note	In the interests of no surprises, a separate, shorter version of this briefing will be sent today to: <ul style="list-style-type: none">• The Minister for National Security and Intelligence• The Minister of Foreign Affairs• The Minister for Trade and Export Growth• The Minister of Broadcasting, Communications and Digital Media	Yes/No

Hon Andrew Little
Minister Responsible for the GCSB
Date: