GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

PO Box 12-209
Wellington 6144
P +64 4 472 6881
F +64 4 499 3701
www.gcsb.govt.nz

[A1710851]

25 June 2018

Daniel Richards
fyi-request-7766-cd6d2bd7@requests.fyi.org.nz

Dear Mr Richards

Official information request for information about written notices sent to Network Operators

I refer to your official information request dated 4 May 2018 for:

- The number of written notices sent to Network Operators under section 51(2) of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) for all of 2017 and 2018 up to the end of April;
- A list of Network Operators who have been sent written notices under section 51(2) of TICSA for all of 2017 and 2018 up to the end of April; and
- The contents of all written notices sent to Network Operators under section 51(2) of TICSA for all of 2017 and 2018 up to the end of April.

Section 51 of TICSA sets out the process for addressing network security risks. Under section 51(2) of TICSA I must provide a written notice to a Network Operator if I become aware of a proposed decision, course of action, or change by a Network Operator that, in my opinion, would, if implemented, raise a network security risk other than a minimal network security risk.

For the period from 1 January 2017 to 30 April 2018, six written notices were sent to Network Operators by the Government Communications Security Bureau (GCSB) under section 51(2) of TICSA.

I am refusing your request for a list of the Network Operators who received written notices from GCSB under the following sections of the Official Information Act 1982 (OIA):

- 9(2)(ba)(i), the withholding of the information is necessary to protect information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied;
- 9(2)(b)(ii), the withholding of the information is necessary to protect information where the making available of the information would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information.

Please find attached the six written notices that GCSB sent to Network Operators under section 51(2) of TICSA between 1 January 2017 and 30 April 2018. Information has been withheld from these notices under one or more of the following sections of the OIA:

- 6(a), where the making available of the information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand;
- 9(2)(a), the withholding of the information is necessary to protect the privacy of natural persons, including that of deceased natural persons;
- 9(2)(b)(ii), the withholding of the information is necessary to protect information where the making available of the information would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information;
- 9(2)(ba)(i), the withholding of the information is necessary to protect information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied; and
- 18(c)(i), the making available of the information requested would be contrary to the provisions of a specified enactment (the Intelligence and Security Act 2017).

Where information is withheld under section 9 of the OIA, we consider that the public interest does not outweigh the decision to withhold this information in this instance.

If you wish to discuss this decision with us, please feel free to contact information@gcsb.govt.nz.

You have the right to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Yours sincerely

Andrew Hampton
Director-General of the GCSB

~~Commercial in confidence~~

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

P
F

PO Box 12-209
Wellington 6144
+64 4 472 6881
+64 4 499 3701
www.gcsb.govt.nz

22 December 2017

[redacted]

Sent Electronically

Dear [redacted]

Notice of network security risk in re: NCSC-TN-2017-347

1. I am writing to you about the notification [redacted] provided on 4 December 2017 under s 48 of the Telecommunications (Interception Capability and Security) Act 2013 (**TICSA**). The notification was made in regard to the [redacted] (our file reference NCSC-TN-2017-347).

2. This notice is provided in accordance with s 51(2) of TICSA.

3. I have completed my consideration of your notification, taking into consideration the factors listed in s 50 of TICSA. I have decided the decision, course of action, or change proposed in the notification would, if implemented, raise a network security risk, as defined in TICSA.

4. In accordance with s 51(1)(b) of TICSA [redacted] must not implement or give effect to the proposed decision, course of action, or change outlined in the notification -

   (i) unless and to the extent that those actions are consistent with or give effect to a proposal or part of a proposal (relating to the proposed decision, course of action, or change) accepted by the Director under s 52 or a direction of the Minister under s 57 on a matter relating to the proposal; or

(ii) unless the Director has referred a matter (arising from the proposal) to the Minister responsible for the Government Communications Security Bureau under s 54 and the Minister does not make a direction in respect of the proposal; or

(iii) unless the Director has notified the network operator that the Director has not accepted the proposal but has decided not to refer the matter to the Minister under s 54.

5. In accordance with s 51(3) of TICSA, [redacted] as soon as practicable, submit a proposal to prevent or sufficiently mitigate the network security risks identified.

6. [redacted] may still be able to proceed with the proposed changes if the risk can be sufficiently mitigated, under s 51(1)(b) of TICSA [redacted] not implement or give effect to the proposal at this stage, given this notice.

7. Once a mitigation proposal has been received, it will be assessed in accordance with s 52 of TICSA.

8. My team would be happy to provide a classified briefing to your cleared staff to provide more information regarding the network security risk identified. We will contact [redacted] to arrange a time. Following that briefing, we will provide a copy of the reasons for the decision (subject to redaction of classified material).

9. I appreciate [redacted] cooperation and assistance with this notification.

Yours sincerely,

[redacted]

GCSB

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

PO Box 12-209
Wellington 6144
P +64 4 472 6881
F +64 4 499 3701
www.gcsb.govt.nz

1 May 2017

[redacted]

Sent Electronically

Dear [redacted]

Notice of network security risk in re: NCSC-TN-2017-235

1. I am writing to you in relation to a notification provided on 1 February 2017 under section 48 of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA). The notification was made in regards to the [redacted] (our file reference NCSC-TN-2017-235).

2. This notice is provided in accordance with s 51(2) of TICSA.

3. I have completed my consideration of your notification taking into consideration the factors listed in s 50 of TICSA. I have decided that the decision, course of action, or change proposed in the notification would, if implemented, raise a significant network security risk, as defined in the Act. A summary of the reasons for my views is set out below. My full reasons for my decision (subject to redaction for classified material) will be provided following a briefing with [redacted] holding a security clearance.

4. Given this notice, you may not proceed with implementing the changes outlined in your notification at this time, and must submit a mitigation proposal. Your TICSA obligations are summarised at the end of this letter.

Consideration of network security risks under s 50 of TICSA

5. I have considered the notification in light of the factors set out in section 50 of TICSA.

6. Section 50 provides that, when considering whether the proposed decision, course of action, or change proposed in the notification would, if implemented, raise a network security risk or significant network security risk under Part 3 of TICSA, I –

   (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) communications services;

(vi) transport services;

(vii) health services;

(viii) education services.

Network security risks raised

7. I consider the changes proposed by the notification would, if implemented, raise a significant network security risk.

8. I consider that the risk of compromise or degradation of [redacted] network, or the impairment of the confidentiality, integrity, or availability of telecommunications on the network is likely for the following reasons:

[redacted]

9. The impact of such events occurring on the provision of services listed in s 50(1)(b) of TICSA would be major, for the following reasons:

a. [redacted] with coverage across New Zealand businesses and critical national services;

b. Section 50(1)(b) services provided within the coverage area include [redacted] used by a number of businesses and government services.

c. [redacted] would likely have flow-on effects to the services provided by [redacted] and end-users and critical national services relying on [redacted].

d. A compromise could have a range of impacts on s 50(1)(b) services, including on the confidentiality, integrity, or availability of telecommunications in relation to those services, or of the ability for those services to be provided.

e. While the impact will vary depending on the actor exploiting the vulnerabilities, the following kinds of harm/loss are possible:

[redacted]

10. [redacted]

Mitigation proposals will be required in accordance with s 51(3) of TICSA

11. In accordance with s 51(1)(b) of TICSA, you must not implement or give effect to the proposed decision, course of action, or change outlined in your notification -

    (i) unless and to the extent that those actions are consistent with or give effect to a proposal or part of a proposal (relating to the proposed decision, course of action, or change) accepted by the Director under section 52 or a direction of the Minister under section 57 on a matter relating to the proposal; or

    (ii) unless the Director has referred a matter (arising from the proposal) to the Minister responsible for the Government Communications Security Bureau under section 54 and the Minister does not make a direction in respect of the proposal; or

    (iii) unless the Director has notified the network operator that the Director has not accepted the proposal but has decided not to refer the matter to the Minister under section 54.

12. In accordance with s 51(3) of the Act, you must, as soon as practicable, submit a proposal to prevent or sufficiently mitigate the network security risks identified.

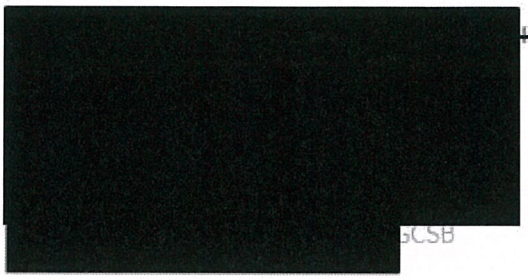
13. While [redacted] still be able to proceed with the proposed changes if the risk can be sufficiently mitigated, under section 51(1)(b) of TICSA [redacted] not implement or give effect to the proposal at this stage, given this notice.

14. Once a mitigation proposal has been received, we will assess that proposal in accordance with s 52 of the Act.

15. I would be happy to provide a classified briefing to [redacted] staff to provide more information regarding the network security risk identified. I will contact [redacted] to arrange a time.

16. I appreciate [redacted] cooperation and assistance with this notification.

Yours sincerely,



GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

PO Box 12-209
Wellington 6144
P +64 4 472 6881
F +64 4 499 3701
www.gcsb.govt.nz

1 May 2017

[redacted]

Sent Electronically

Dear [redacted]

Notice of network security risk in re: NCSC-TN-2017-243

1. I am writing to you in relation to a notification provided on 21 February 2017 under section 48 of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA). The notification was made in regards to the [redacted] our file reference NCSC-TN-2017-243).

2. This notice is provided in accordance with s 51(2) of TICSA.

3. I have completed my consideration of your notification taking into consideration the factors listed in s 50 of TICSA. I have decided that the decision, course of action, or change proposed in the notification would, if implemented, raise a significant network security risk, as defined in the Act. A summary of the reasons for my views is set out below. My reasons for this decision (subject to redaction for classified material) will be provided following a briefing with [redacted] holding a security clearance.

4. Given this notice, you may not proceed with implementing the changes outlined in your notification at this time, and must submit a mitigation proposal. Your TICSA obligations are summarised at the end of this letter.

Consideration of network security risks under s 50 of TICSA

5. I have considered the notification in light of the factors set out in section 50 of TICSA.

6. Section 50 provides that, when considering whether the proposed decision, course of action, or change proposed in the notification would, if implemented, raise a network security risk or significant network security risk under Part 3 of TICSA, I –

   (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) communications services:

(vi) transport services:

(vii) health services:

(viii) education services.

Network security risks raised

7. I consider the changes proposed by the notification would, if implemented, raise a significant network security risk.

8. I consider that the risk of compromise or degradation of [redacted] network, or the impairment of the confidentiality, integrity, or availability of telecommunications on the network is likely for the following reasons:

[redacted]

9. A risk eventuating would have a moderate effect on the provision of services listed in s 50(1)(b) of TICSA, for the following reasons:

a. [redacted] with coverage across New Zealand businesses and critical national services.

b. Section 50(1)(b) services provided within the coverage area include [redacted], used by a number of businesses and government services.

c. [redacted] would likely have flow-on effects to the services provided by [redacted] and end-users and critical national services relying on [redacted].

d. A compromise could have a range of impacts on s 50(1)(b) services, including on the confidentiality, integrity, or availability of telecommunications in relation to those services, or of the ability for those services to be provided.

e. While the impact will vary depending on the actor exploiting the vulnerabilities, the following kinds of harm/loss are possible:

[redacted]

[redacted]

10. [redacted]

Mitigation proposals will be required in accordance with s 51(3) of TICSA

11. In accordance with s 51(1)(b) of TICSA, you must not implement or give effect to the proposed decision, course of action, or change outlined in your notification -

    (i) unless and to the extent that those actions are consistent with or give effect to a proposal or part of a proposal (relating to the proposed decision, course of action, or change) accepted by the Director under section 52 or a direction of the Minister under section 57 on a matter relating to the proposal; or

    (ii) unless the Director has referred a matter (arising from the proposal) to the Minister responsible for the Government Communications Security Bureau under section 54 and the Minister does not make a direction in respect of the proposal; or

    (iii) unless the Director has notified the network operator that the Director has not accepted the proposal but has decided not to refer the matter to the Minister under section 54.

12. In accordance with s 51(3) of the Act, you must, as soon as practicable, submit a proposal to prevent or sufficiently mitigate the network security risks identified.

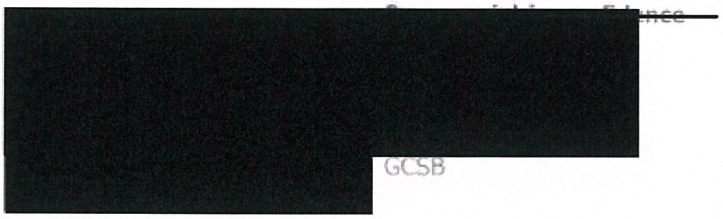
13. [redacted] may still be able to proceed with the proposed changes if the risk can be sufficiently mitigated, under section 51(1)(b) of TICSA [redacted] not implement or give effect to the proposal at this stage, given this notice.

14. Once a mitigation proposal has been received, I will assess that proposal in accordance with s 52 of the Act.

15. I would be happy to provide a classified briefing [redacted] staff to provide more information regarding the network security risk identified. I will contact [redacted] arrange a time.

16. I appreciate [redacted] cooperation and assistance with this notification.

Yours sincerely,



GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

PO Box 12-209
Wellington 6144
P +64 4 472 6881
F +64 4 499 3701
www.gcsb.govt.nz

1 May 2017

[redacted]

Sent Electronically

Dear [redacted]

Notice of network security risk in re: NCSC-TN-2017-244

1. I am writing to you in relation to a notification provided on 21 February 2017 under section 48 of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA). The notification was made in regards to the [redacted] (our file reference NCSC-TN-2017-244).

2. This notice is provided in accordance with s 51(2) of TICSA.

3. I have completed my consideration of your notifications taking into consideration the factors listed in s 50 of TICSA. I have decided that the decision, course of action, or change proposed in the notification would, if implemented, raise a significant network security risk, as defined in the Act. A summary of the reasons for my views is set out below. My full reasons for this decision (subject to redaction for classified material) will be provided following a briefing with [redacted] holding a security clearance.

4. Given this notice, you may not proceed with implementing the changes outlined in your notification at this time, and must submit a mitigation proposal. Your TICSA obligations are summarised at the end of this letter.

Consideration of network security risks under s 50 of TICSA

5. I have considered the notification in light of the factors set out in section 50 of TICSA.

6. Section 50 provides that, when considering whether the proposed decision, course of action, or change proposed in the notification would, if implemented, raise a network security risk or significant network security risk under Part 3 of TICSA, I –

(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) communications services:

(vi) transport services:

(vii) health services:

(viii) education services.

Network security risks raised

7. I consider the changes proposed by the notification would, if implemented, raise a significant network security risk.

8. I consider that the risk of compromise or degradation of [redacted] network, or the impairment of the confidentiality, integrity, or availability of telecommunications on the network is likely for the following reasons:

[redacted]

9. A risk eventuating would have a major effect on the provision of services listed in s 50(1)(b) of TICSA, for the following reasons:

a. [redacted] with coverage across New Zealand businesses and critical national services.

b. Section 50(1)(b) services provided within the coverage area include [redacted] used by a number of businesses and government services.

c. [redacted] would likely have flow-on effects to the services provided by [redacted] and end-users and critical national services relying on [redacted]

d. A compromise could have a range of impacts on s 50(1)(b) services, including on the confidentiality, integrity, or availability of telecommunications in relation to those services, or of the ability for those services to be provided.

e. While the impact will vary depending on the actor exploiting the vulnerabilities, the following kinds of harm or loss are possible:

10. [redacted]

Mitigation proposals will be required in accordance with s 51(3) of TICSA

11. In accordance with s 51(1)(b) of TICSA, you must not implement or give effect to the proposed decision, course of action, or change outlined in your notification -

    (i) unless and to the extent that those actions are consistent with or give effect to a proposal or part of a proposal (relating to the proposed decision, course of action, or change) accepted by the Director under section 52 or a direction of the Minister under section 57 on a matter relating to the proposal; or

    (ii) unless the Director has referred a matter (arising from the proposal) to the Minister responsible for the Government Communications Security Bureau under section 54 and the Minister does not make a direction in respect of the proposal; or

    (iii) unless the Director has notified the network operator that the Director has not accepted the proposal but has decided not to refer the matter to the Minister under section 54.

12. In accordance with s 51(3) of the Act, you must, as soon as practicable, submit a proposal to prevent or sufficiently mitigate the network security risks identified.

13. [redacted] may still be able to proceed with the proposed changes if the risk can be sufficiently mitigated, under section 51(1)(b) of TICSA [redacted] must not implement or give effect to the proposal at this stage, given this notice.

14. Once a mitigation proposal has been received, I will assess that proposal in accordance with s 52 of the Act.

15. I would be happy to provide a classified briefing to [redacted] staff to provide more information regarding the network security risk identified. I will contac[redacted] to arrange a time.

16. I appreciate [redacted] cooperation and assistance with this notification.

Yours sincerely,

[redacted]

GCSB

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

PO Box 12-209
Wellington 6144
P +64 4 472 6881
F +64 4 499 3701
www.gcsb.govt.nz

09/06/2017

[redacted]

Sent Electronically

Dear [redacted]

Notice of network security risk in re: NCSC-TN-2016-230

1. I am writing to you about the notification [redacted] provided on 30 November 2016 under s 48 of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA). The notification was made about the [redacted] (our file reference NCSC-TN-2016-230).

2. This notice is provided in accordance with s 51(2) of TICSA.

3. I have completed my consideration of your notification, taking into consideration the factors listed in s 50 of TICSA. I have decided the decision, course of action, or change proposed in the notification would, if implemented, raise a significant network security risk, as defined in TICSA. A summary of the reasons for my decision is set out below. A full copy of my reasons (subject to redaction of classified material) will be provided following a briefing with [redacted] holding a security clearance.

4. Given this notice [redacted] may not proceed with implementing the changes outlined in the notification at this time, and must submit a mitigation proposal [redacted] TICSA obligations are summarised at the end of this letter.

Consideration of network security risks under s 50 of TICSA

5. I have considered the notification in light of the factors set out in s 50 of TICSA.

6. Section 50 provides that, when considering whether the proposed decision, course of action, or change proposed in the notification would, if implemented, raise a network security risk or significant network security risk under Part 3 of TICSA, we -

   (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) communications services:

      (vi) transport services:

      (vii) health services:

      (viii) education services.

Network security risks raised

7. I consider the changes proposed by the notification would, if implemented, raise a significant network security risk.

8. My principal concern is [redacted]

9. I consider that the compromising or degrading of the public telecommunications network, and the impairment of the confidentiality, availability, and integrity of telecommunications across the network [redacted]

10. The at-risk systems are the [redacted]

11. [redacted]

12. [redacted]

13. [redacted]

14. [redacted]

15. [redacted] Such activity could be undertaken for a variety of purposes contrary to New Zealand's national security, including New Zealand's economic well-being.

16. [redacted]

Mitigation proposals will be required in accordance with s 51(3) of TICSA

17. In accordance with s 51(1)(b) of TICSA [redacted] must not implement or give effect to the proposed decision, course of action, or change outlined in the notification -

(i) unless and to the extent that those actions are consistent with or give effect to a proposal or part of a proposal (relating to the proposed decision, course of action, or change) accepted by the Director under s 52 or a direction of the Minister under s 57 on a matter relating to the proposal; or

(ii) unless the Director has referred a matter (arising from the proposal) to the Minister responsible for the Government Communications Security Bureau under s 54 and the Minister does not make a direction in respect of the proposal; or

(iii) unless the Director has notified the network operator that the Director has not accepted the proposal but has decided not to refer the matter to the Minister under s 54.

18. In accordance with s 51(3) of TICSA [redacted] as soon as practicable, submit a proposal to prevent or sufficiently mitigate the network security risks identified.

19. [redacted] may still be able to proceed with the proposed changes if the risk can be sufficiently mitigated, under s 51(1)(b) of TICSA [redacted] must not implement or give effect to the proposal at this stage, given this notice.

20. Once a mitigation proposal has been received, I will assess that proposal in accordance with s 52 of TICSA.

21. My team would be happy to provide a classified briefing to [redacted] staff to provide more information regarding the network security risk identified. We will contact [redacted] to arrange a time.

22. I appreciate [redacted] cooperation and assistance with this notification.

Yours sincerely,

[redacted]

GCSB

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

PO Box 12-209
Wellington 6144
P +64 4 472 6881
F +64 4 499 3701
www.gcsb.govt.nz

09/06/2017

[redacted]

Sent Electronically

Dear [redacted]

Notice of network security risk in re: NCSC-TN-2017-254

1. I am writing to you about the notification provided by [redacted] on 28 February 2017 under s 48 of the Telecommunications (Interception Capability and Security) Act 2013 (**TICSA**). The notification was made of a proposal to [redacted] (our file reference NCSC-TN-2017-254).

2. This notice is provided in accordance with s 51(2) of TICSA.

3. I have completed my consideration of the notification taking into consideration the factors listed in s 50 of TICSA. I have decided the decision, course of action, or change proposed in the notification would, if implemented, raise a significant network security risk, as defined in TICSA. A summary of the reasons for my decision is set out below. A full copy of my reasons (subject to redaction of classified material) will be provided following a briefing with [redacted] holding a security clearance.

4. Given this notice, [redacted] may not proceed with implementing the changes outlined in the notification at this time, and must submit a mitigation proposal [redacted] TICSA obligations are summarised at the end of this letter.

Consideration of network security risks under s 50 of TICSA

5. I have considered the notification in light of the factors set out in s 50 of TICSA.

6. Section 50 provides that, when considering whether the proposed decision, course of action, or change proposed in the notification would, if implemented, raise a network security risk or significant network security risk under Part 3 of TICSA, we –

   (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) communications services:

      (vi) transport services:

      (vii) health services:

      (viii) education services.

Network security risks raised

7. I consider the changes proposed by the notification would, if implemented, raise a significant network security risk.

8. I consider that the compromising or degrading of the public telecommunications network, and the impairment of the confidentiality, availability, and integrity of telecommunications across the network, is likely given:

[redacted]

9. [redacted]

10 [redacted]

[redacted]

16. A compromise of these systems could have a critical effect on the provision of services listed in s 50(1)(b) of TICSA. Among the services listed in s 50(1)(b) which would be affected are [redacted]

17. A threat actor would be able to undertake [redacted] could be used for a variety of purposes contrary to New Zealand's national security, including its economic well-being.

Mitigation proposals will be required in accordance with s 51(3) of TICSA

18. In accordance with s 51(1)(b) of TICSA [redacted] must not implement or give effect to the proposed decision, course of action, or change outlined in the notification -

    (i) unless and to the extent that those actions are consistent with or give effect to a proposal or part of a proposal (relating to the proposed decision, course of action, or change) accepted by the Director under s 52 or a direction of the Minister under s 57 on a matter relating to the proposal; or

    (ii) unless the Director has referred a matter (arising from the proposal) to the Minister responsible for the Government Communications Security Bureau under s 54 and the Minister does not make a direction in respect of the proposal; or

    (iii) unless the Director has notified the network operator that the Director has not accepted the proposal but has decided not to refer the matter to the Minister under s 54.

19. In accordance with s 51(3) of TICSA [redacted] must, as soon as practicable, submit a proposal to prevent or sufficiently mitigate the network security risks identified.

20. [redacted] may still be able to proceed with the proposed changes if the risk can be sufficiently mitigated, under s 51(1)(b) of TICSA [redacted] must not implement or give effect to the proposal at this stage, given this notice.

21. Once a mitigation proposal has been received, I will assess that proposal in accordance with s 52 of TICSA.

22. My team would be happy to provide a classified briefing to [redacted] leared staff to provide more information regarding the network security risk identified. We will contact [redacted] to arrange a time.

23. I appreciate [redacted] cooperation and assistance with this notification.

Yours sincerely,

[redacted]

GCSB