Public Engagement Report

1. The Intelligence and Security Act 2017 (the Act) sets out the objectives, functions and powers of New Zealand's intelligence and security agencies: The New Zealand Security Intelligence Service (NZSIS), and the Government Communications Security Bureau (GCSB).

2. The Act sets out safeguards and human rights protections, including oversight bodies such as the Inspector-General of Intelligence, the Intelligence and Security Committee, and the Commissioners of Security Warrants. The Act requires the intelligence and security agencies to act in accordance with New Zealand's human rights obligations and in a professional and politically neutral way.

3. Section 235 of the Act requires periodic reviews to be undertaken every five to seven years. The Terms of Reference for this review were published in March 2022 and set out the purpose of the review, matters to have particular regard to, matters to take into account when conducting the review, expectations on public engagement and deliverables.

4. This report summarises key findings from the online public engagement survey conducted for the review.

Overview of Engagement

5. Public engagement for the review of the Act was held for a period of two months, between 1 August 2022 and 30 September 2022. Targeted engagement began earlier in April 2022 and continued through to October 2022. The reviewers thank all those who participated through online and email submissions, meetings, and workshops.

Purpose

6. The purpose of the public engagement was to:

- ensure that participants from affected communities had an opportunity to provide input and influence the findings and recommendations of the review; and
- obtain public feedback on three key areas of the Act:
    - the **extent of the intelligence and security agencies' powers**;
    - **limits and controls** on the agencies; and
    - **public participation and transparency** related to the agencies and national security more generally.

Limitations

7. The timeframe for the review, and the impact of COVID-19 on the work of the review team, influenced the public engagement process. Although the review team endeavoured to meet in-person with as many people as possible, it has also held virtual meetings and requested that people provide their views in writing.

8. Significant reliance on an online and digital engagement approach constrained public engagement. However, face-to-face meetings, hui and administering the survey in-person proved to be effective for public engagement.

Content and methodology

9. Engagement resources covered high-level information about the Act and the review. The engagement sought public feedback on the three key areas listed in paragraph 6.

10. The engagement information was incorporated into the following materials:

- website content;
- a press release from the reviewers;
- a survey on *Citizen Space* – the Ministry of Justice's consultation hub;
- social media posts;
- an informative video to promote engagement; and
- an overview email for targeted engagement, inviting participation and feedback.

11. In preparing for public engagement, the review sought input from research and communications officials to ensure areas of interest were communicated to the public in a way that maximised feedback. Engagement was promoted through a range of channels, including through:

- email and via stakeholder networks;
- social media (eg, Ministry of Justice LinkedIn, Twitter and Facebook accounts, and stakeholder social media accounts); and
- the Ministry of Justice website.

12. This engagement approach was developed in accordance with the public sector Policy Community Engagement Tool.[1]

Participation

13. In terms of participation, the review engaged the following:

- a total of 119 responses to the online survey via *Citizen Space*;
- a total of 24 submissions via email, across both the public and targeted engagement timeframes; and
- twenty separate meetings, involving approximately 90 people. A small number of these meetings occurred just outside the public engagement timeframe due to scheduling requirements.

[1] The public engagement approach was undertaken in accordance with the 'consult' level of engagement on the IAP2 spectrum, with the intention to listen and obtain feedback from key stakeholders and communities, and the general public. For more detail, see: "Policy Community Engagement Tool," *The Policy Project*, New Zealand Government, (January 2022), p. 5.

14. Overall, more than 230 people participated in the public engagement, with the email submissions often reflecting organisations comprising numerous employees, customers and stakeholders who are not included in this number.

15. Given the complexity of the content of the review (and survey tool), the ability to discuss the intent of the questions face-to-face through various meetings and hui proved to be effective in attaining public participation.

Key findings from the online *Citizen Space* survey

16. The public engagement aimed to ensure that:

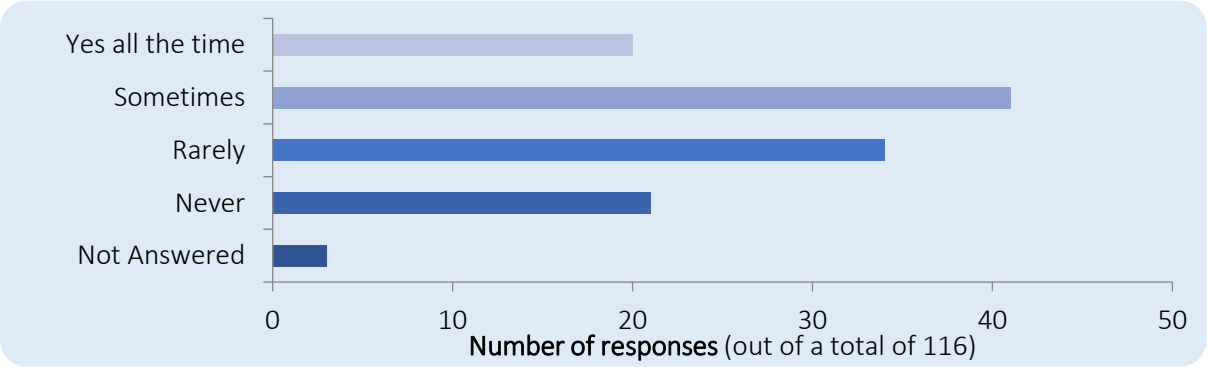
- the reviewers could understand the public's views on the agencies' powers to protect New Zealand's free, open and democratic society; and
- participants from affected communities have an opportunity to provide input and influence review findings and recommendations.

17. The public engagement insights are set out against the three key areas (see paragraph 6) and summarise themes that emerged primarily from the online surveys and email submissions. The themes are not intended to reflect all feedback provided through engagement, particularly where feedback was only provided by a single or very few participants. The survey responses are not a representative sample.

Extent of the intelligence and security agencies' power

18. Sixty-one participants (51 per cent) noted that it was okay for the intelligence and security agencies to collect information for the purposes of identifying and assessing national security risks, either "all of the time" or "sometimes". Fifty-five participants (46 per cent) noted that it was "rarely" or "never" okay to collect information for this purpose. See responses to Question 1 below.

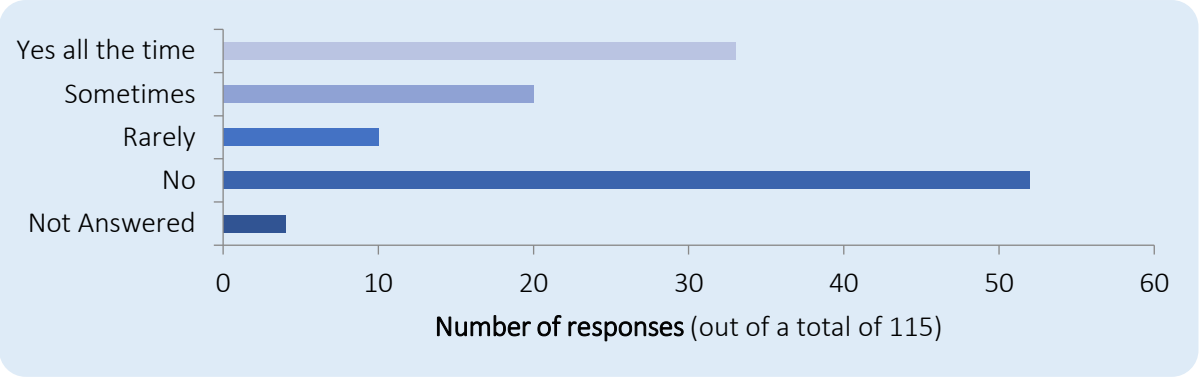
<u>Question 1:</u> Is it okay for the NZSIS and GCSB to collect information on anyone to help them identify and assess national security risks for keeping New Zealand safe?



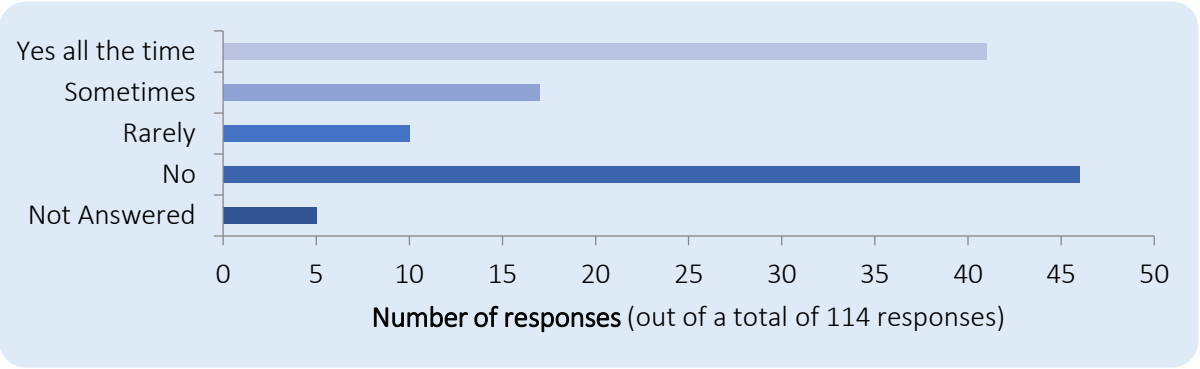
19. In response to Question 3 (below) the majority of participants noted that it was not important that New Zealanders have more protections compared to non-New Zealanders when intelligence and security agencies were collecting information for national security risks or to fulfil other statutory obligations. However, in response to Question 5 on collecting information on international relations and economic well-being (further below), the number of participants who indicated "yes

all the time" was higher while those that responded "no" or "sometimes" was lower than Question 3.

Question 3: When agencies collect information to identify and assess national security risks, is it important that New Zealanders have more protections compared to non-New Zealanders?



Question 5: In addition to collecting information to protect national security, agencies can collect information to support their other statutory objectives which are to contribute to New Zealand's international relations and well-being and economic well-being. Is it important that New Zealanders have more protections compared to non-New Zealanders when agencies collect information to meet these objectives?



20. Participants in favour of greater protections for New Zealanders over non-New Zealanders cited the State's duty to protect citizens with regard to their rights, and against threats. Participants who did not favour greater protections for New Zealanders over non-New Zealanders tended to indicate either:

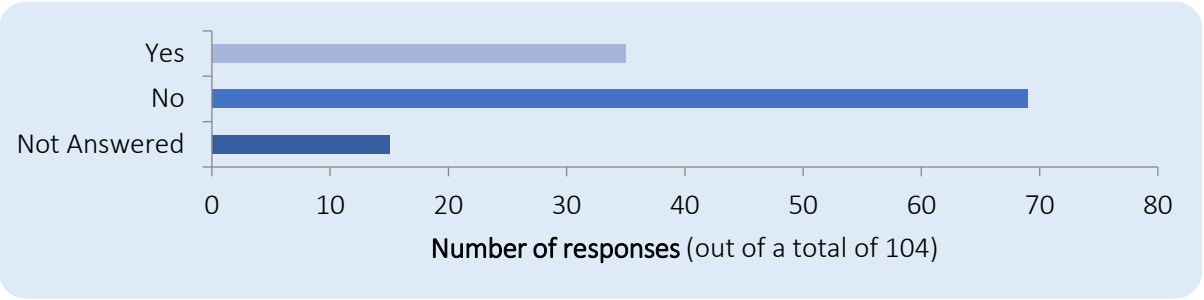
- that risks to national security come from overseas and domestically, so it is important to protect New Zealanders as well as non-New Zealanders; or
- human rights and the right to privacy are universal, regardless of national origin.

21. Forty-two participants thought they would feel more protected, and an equal 42 participants thought they would feel less protected if the NZSIS and GCSB collected information that is openly available on the internet (including about the participants or the people in their communities) to help the agencies identify potential risks and threats to New Zealand that they did not know about. Twenty-nine participants did not know if they would feel more or less protected.

Limits and controls on the intelligence and security agencies

22. Sixty-nine participants (58 per cent) noted that the Act does not have the balance right between security and interests and the rights and freedoms of New Zealanders. See responses to Question 9 below.

Question 9: Do you think the Act has the right balance between security interests and the rights and freedoms of New Zealanders?



23. Sixty-nine per cent of respondents indicated that the security and intelligence agencies were not sufficiently open with the public about their activities.

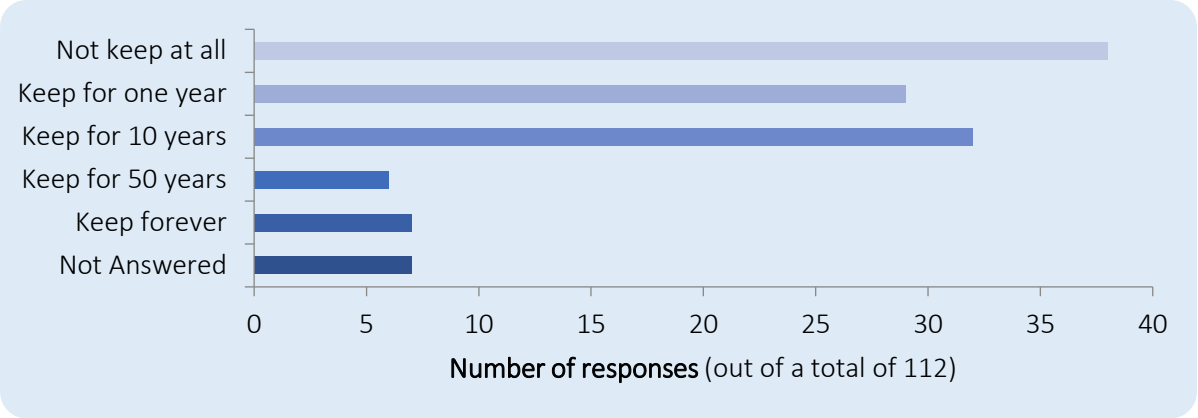
24. To address this, some participants suggested having the Intelligence and Security Committee behave more like a select committee and receive regular submissions from the public and openly question agency heads or create a new independent oversight body and/or improved governance of the intelligence system.

25. Other suggestions made by participants to improve to the Act, include:

- recognising the Treaty of Waitangi/Te Tiriti o Waitangi;
- clearly defining the role of information sharing between the intelligence and security agencies and other domestic Government agencies;
- considering issues relating to the overall intelligence community rather than just the NZSIS and GCSB (such as New Zealand Police and Ministry for Foreign Affairs and Trade); and
- increasing public reporting and implementing more limitations and controls on the agencies to prevent abuse of power.

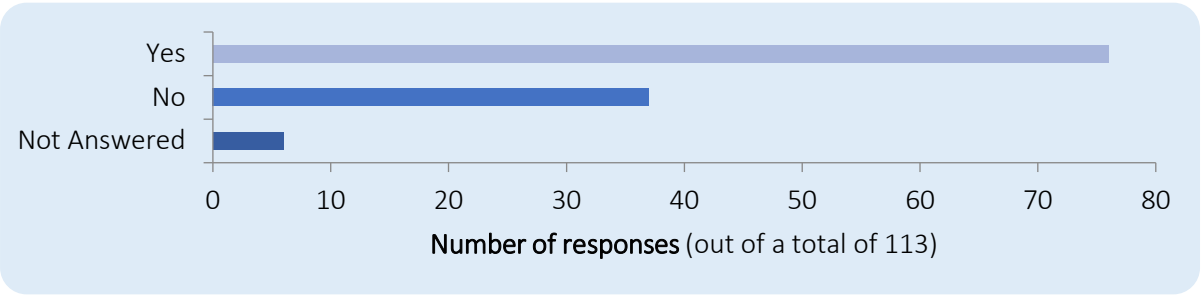
26. Although the majority of participants noted that it was okay for the intelligence and security agencies to collect information for the purposes of identifying and assessing national security risks, either "all of the time" or "sometimes", 67 participants (56 per cent) thought that agencies should not be able to retain information collected for longer than one year, or at all. This is despite the question noting that the information could be important to future work by the agencies. See responses to question 15 below.

<u>Question 15:</u> If an agency collects information under a warrant that is irrelevant to its work now, but could possibly be important in the future how long should the agencies be able to keep this information?



27. Seventy-six participants (64 per cent) thought that intelligence agencies should be able to investigate people that express extremist views when exercising their right to freedom of speech. See responses to Question 11 below.

<u>Question 11:</u> Should intelligence agencies be able to investigate people who express extremist views (as an exercise of their right of free speech)?



Public participation

28. The majority of participants did not believe that they had enough information about the agencies and oversight mechanisms to feel confident that they were working appropriately.

29. To support greater public awareness of the intelligence and security agencies, and input into national security issues, participants identified the need for Government to increased public consultation, awareness advertising and information to educate people about issues and how to get involved. Some participants also indicated that the public also needed to take a more active interest and role in national security discussions. This could be supported by agencies which could also provide a means for safe and confidential options for the community to report concerns.

30. Participants were asked to rank a list of four types of activities from most important to least important in terms of what the NZSIS and GCSB should focus on. Fifty-six participants (47 per cent) indicated that terrorism and violent extremism as most important, 19 participants (16 per cent) indicated that foreign interference and espionage as most important, 18 participants (15 per cent) indicated malicious cyber activity (eg, hacking, ransomware etc) as most important, and 16

participants indicated specific types of crime (eg, transnational, serious, and organised) as most important.

31. Participants also raised a number of other risks that are important for the agencies to consider, including social well-being changes such as homelessness, racism and incitement of hatred; technology-related issues; environmental issues; the economy; and issues with domestic state agencies such as a lack of transparency or collaboration with overseas intelligence agencies, institutional racism and no recognition of Te Tiriti o Waitangi.