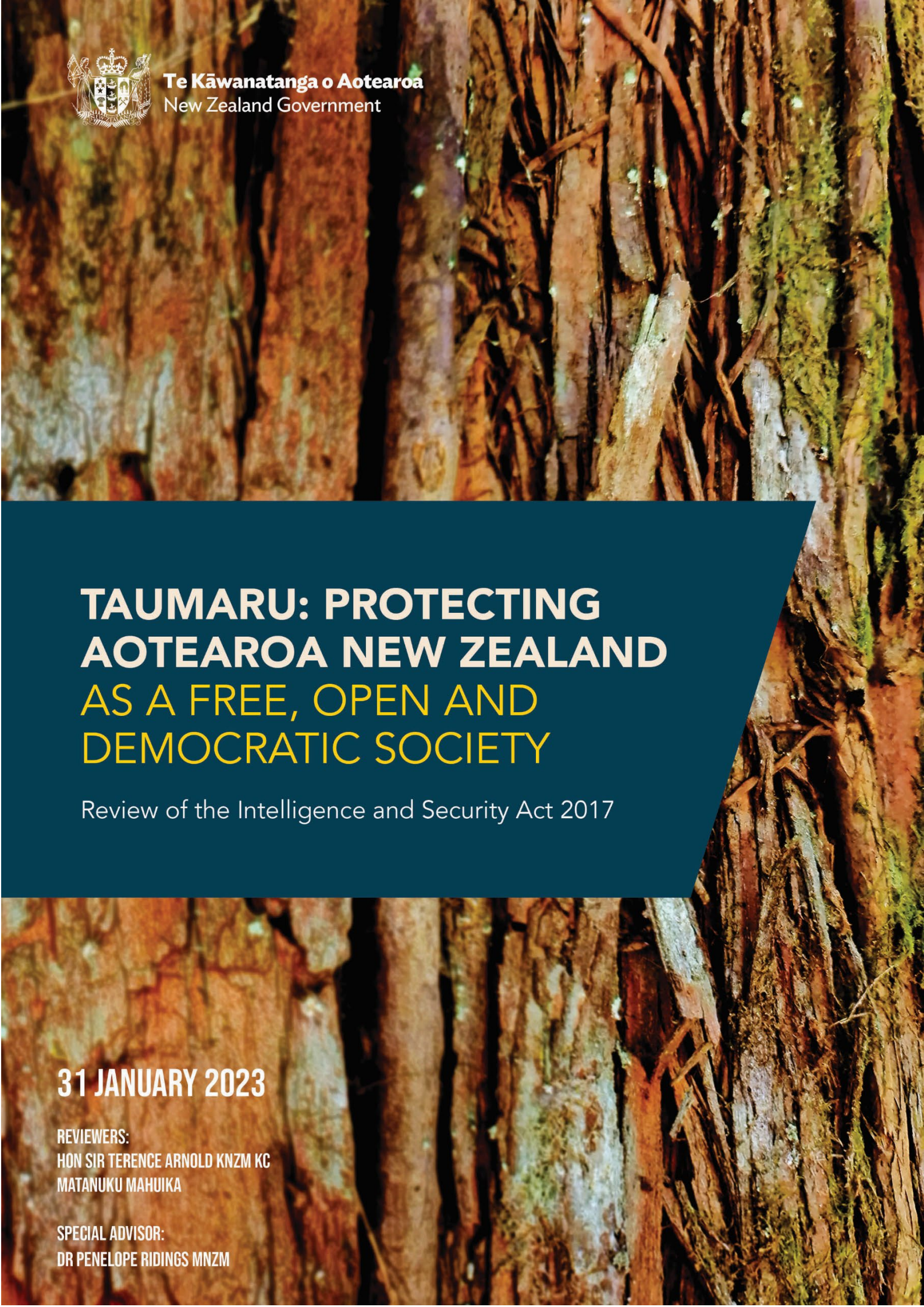


Te Kāwanatanga o Aotearoa
New Zealand Government

TAUMARU: PROTECTING AOTEAROA NEW ZEALAND AS A FREE, OPEN AND DEMOCRATIC SOCIETY

Review of the Intelligence and Security Act 2017

31 JANUARY 2023

REVIEWERS:
HON SIR TERENCE ARNOLD KNZM KC
MATANUKU MAHUIKA

SPECIAL ADVISOR:
DR PENELOPE RIDINGS MNZM

This document may be cited as: Hon Sir Terence Arnold KNZM KC and Matanuku Mahuika (2023) *Taumaru: Protecting Aotearoa New Zealand as a free, open and democratic society*. Wellington: Ministry of Justice.

Ministry of Justice
SX10088
Wellington
https://www.justice.govt.nz/

ISBN: 978-0-473-67010-8 (print)
ISBN: 978-0-473-67010-8 (PDF)

Foreword

In the foreword to the 2016 report of their review of the previous legislation governing the intelligence and security agencies, Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM, said that the new Intelligence and Security Act 2017 "should state clearly that its fundamental purpose is the protection of New Zealand as a free, open, and democratic society". They went on to describe that principle as "the guiding principle by which the activities of the Agencies must be undertaken and judged".

Section 3 of the Act does clearly state this guiding principle. We have attempted to follow it in the present review. In particular, we have sought to understand what a free, open and democratic New Zealand looks like today, and to place the Act and the intelligence and security agencies firmly in that setting.

Now, seven years after the Cullen/Reddy review, we believe several significant changes to the Act are needed. They are required to ensure the Act is 'fit for purpose' and remains true to the guiding principle of protecting New Zealand as a free, open and democratic society.

Like Sir Michael and Dame Patsy, we have been exposed to a wide range of views about the intelligence and security agencies during our review. But interestingly no one argued that New Zealand did not need intelligence and security agencies.

Rather, the issues raised related to matters such as the lack of transparency about the agencies' activities; concerns about the effectiveness of control and oversight mechanisms (including the lack of a rigorous process for assessing the agencies' effectiveness); whether the Act and the agencies adequately reflect New Zealand's diverse and multi-cultural society; and legislative gaps and inconsistencies that appear when the intelligence and security community is considered as a whole, some of which affect the operation of the Act.

The review has been rather more demanding and time-consuming than we initially envisaged. Like everything else, it has been affected by COVID-19. However, for both of us, the review has, despite its challenges, been a fascinating, informative and rewarding experience. We feel we have produced something of value, and hope that proves to be the case.

As we indicate in the report, we consulted widely during the review, both within and outside the public sector, and found that invaluable. We are very grateful to all those who took the time to share their views, knowledge and expertise with us. We should mention the significant assistance and cooperation we have received from the Department of the Prime Minister and Cabinet, the Government Communications Security Bureau, the New Zealand Security Intelligence Service and the Inspector-General of Intelligence and Security. We did not always agree, but the discussion and debate helped us formulate, test and sharpen our ideas.

We also record our gratitude to the non-governmental organisations we consulted, including Kāpuia. Representatives of these organisations are generally volunteers and while they value the opportunity to express their views, consultation does impose a significant burden on them. We acknowledge that. We also acknowledge that we gained valuable insights from our discussions with them.

Under the Act, the Ministry of Justice was responsible for providing administrative, secretarial and other necessary support to the review. We express our gratitude to the members of the Ministry team who supported us: our initial manager, Tania Chin, whose preparatory and other analytical work became a 'go to' resource; her replacement from July 2022, Virginia McLean, whose formidable organisational skills ensured we made timely progress; Letitia Garrett and Jason Lescelius,

who provided critical support and input throughout the review. We also acknowledge the valuable assistance given by outside contractors: Mike Seddon, who provided much needed technical expertise; Jody Hamilton, who coordinated the public consultation process; Nicola Hill, who undertook research and other work as the report was being written; and Savita Parbhu, who provided secretarial services.

Finally, we must acknowledge publicly that we would not have been able to complete this review as we have without our special adviser, Dr Penelope Ridings. While Dr Ridings has been closely involved in all aspects of our work, she has taken particular responsibility for issues relating to the collection, storage, use, sharing and disposal of information by the agencies. Her commitment to the work of the review and the quality of her input (particularly, her command of the detail) has been truly outstanding and we are greatly indebted to her.

We have titled our report: *Taumaru: Protecting Aotearoa New Zealand as a free, open and democratic society*. The word 'Taumaru' means to protect or shelter. It captures in a simple and succinct way the reason for the Agencies and, indeed, our security and intelligence apparatus in general. The second part of the title, 'Protecting New Zealand as a free, open and democratic society' captures that same sentiment. It also points to a fundamental challenge arising from the existence of the Agencies, in acting to maintain a free, open and democratic society we must be careful to ensure we do not undermine those same values.

I orea te tuatara ka puta ki waho – A problem is solved by continuing to find solutions.

Hon Sir Terence Arnold KNZM KC

Matanuku Mahuika

Contents

EXECUTIVE SUMMARY

Executive summary

E.1. The purpose of this review was to:

- determine whether improvements should be made to the Intelligence and Security Act 2017 (ISA) "to ensure it continues to be effective, clear and fit for purpose"
- "consider the recommendations and issues related to [the ISA] that were raised in the Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain".

E.2. The ISA was enacted following recommendations made by Sir Michael Cullen and Dame Patsy Reddy in their 2016 report following their review (the Cullen/Reddy review) of earlier legislation governing the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) (referred to in our report as 'the Agencies').

E.3. Our review is the first to be carried out under the ISA and was not intended to be a fundamental or 'first principles' review. In addition, it was carried out against the background that the Department of the Prime Minister and Cabinet (DPMC) has been undertaking work on the overarching national security policy settings, including the structure and current separation of the Agencies. In our review, we were directed to be aware of that work but not replicate it. Additionally, it is important to note that our review is of the ISA and not of the Agencies themselves.

Setting for the review

E.4. The review took place against the backdrop of:

- a significant challenge to world order in the form of Russia's invasion of Ukraine, which highlighted the need for good intelligence to inform decision-making
- rapid technological developments, which are profoundly influencing the way New Zealanders live their lives, and the way intelligence and security agencies operate.

E.5. To explain the second point, the combination of developments in mobile phone technology, the internet and the World Wide Web (including the proliferation of internet-enabled devices and the rapid expansion of web-based services, and social media) have led to people increasingly living their lives 'on line' and, effectively, in public view (our images are routinely captured in many facets of our daily lives).

E.6. Digitisation and the extraordinary volume of data produced every day have resulted in the development of technologies to collect, examine, manipulate and utilise that data. Companies have been quick to exploit the opportunities that online life has presented in terms of acquiring, aggregating, interrogating and analysing data, with a view to producing material that can be monetised or otherwise used for commercial purposes.

E.7. There are many benefits to society generally from these developments. For example, they have enhanced freedom of expression, encouraged global debate and enabled greater democratic participation. But they have also created challenges, for example, by creating opportunities for malicious actors to mount cyber-attacks, conduct disinformation campaigns and undermine (or potentially undermine) privacy in a variety of ways.

E.8. Similarly, these developments can assist the work of intelligence and security agencies by giving them access to an almost infinite range of data and providing the analytical tools to deal with

that data. But, equally, those same developments can make the agencies' work more difficult, for example, as a result of the widespread use of encryption and virtual private networks.

E.9. Commentators have suggested that rapid technological developments have opened up commercial opportunities that are leading to a paradigm shift in the way intelligence and security agencies work internationally. This is because such agencies are able to make increasing use of commercially and publicly available data in their work. Some commentators argue that further regulation may be needed in this area.

The limited scope of the Intelligence and Security Act

E.10. The intelligence and national security system in Aotearoa New Zealand continues to lack cohesion from a legal point of view. To the extent that New Zealand can be said to have an intelligence and national security system, the ISA does not address it as a whole. Rather, the Act deals with several core components, specifically the GCSB, the NZSIS and, to a limited extent, the National Assessments Bureau within DPMC. Other important elements of the intelligence and national security community, such as the intelligence functions within the New Zealand Defence Force (NZDF), the New Zealand Police (Police) and the New Zealand Customs Service (Customs), are mentioned only peripherally in the ISA or not at all.

E.11. In relation to the GCSB and the NZSIS, the ISA sets out their objectives, functions, powers and oversight mechanisms. It requires these two Agencies to cooperate with each other and with the NZDF and the Police, but it does not deal with the functions and powers of the NZDF and the Police in the intelligence/national security context.

E.12. Moreover, the legislation governing organisations such as the NZDF, Police and Customs does not reflect their intelligence gathering and national security roles, which means that, in some instances, they have had to develop 'work-arounds' in conjunction with the Agencies to enable them to contribute more fully and effectively to intelligence gathering and national security activities.

Our approach

E.13. For this review, we have been briefed by, and/or consulted widely with, the Agencies; DPMC; those performing oversight functions under the ISA (the Inspector-General of Intelligence and Security, Commissioners of Intelligence Warrants and Parliament's Intelligence and Security Committee); government departments and other agencies that have intelligence gathering and national security functions or interests; other oversight officials such as the Auditor-General, the Ombudsman, the Privacy Commissioner, the Human Rights Commissioner and the Independent Police Conduct Authority; academics; Kāpuia (the ministerial advisory group on the government's response to the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain (the Royal Commission)); professional, faith-based and ethnic groups; and members of the general public. We have also spoken to oversight officials from Australia, Canada and the United Kingdom and have conducted our own literature research.

E.14. The Royal Commission strongly supported more public discussion of issues relating to national security, and we have applied that principle in writing our report. For that reason, we have attempted to provide enough background material to provide context and make the discussion of the issues understandable to lay readers.

Our recommendations

E.15. This is the first review carried out under the ISA, and as such, many of the recommendations we make are of a routine, technical nature. These routine recommendations are set out in appendix C to this report.

E.16. There are also other recommendations of more significance. The three major ones are:

- including a definition of "protection of national security" in the ISA
- removing the distinction between Type 1 and Type 2 warrants
- reforming Parliament's Intelligence and Security Committee.

Including a definition of "protection of national security" in the ISA

E.17. There is currently no definition of "national security" in the ISA, despite the fact that the Cullen/Reddy review recommended there be one. We recommend that s 4 of the ISA (Interpretation) be amended to include a definition of "protection of national security".

E.18. We make this recommendation because "national security", and the "protection of national security" in particular, plays a central role in the scheme of the ISA. So, for example, s 3(a) of the ISA (Purpose) provides:

> The purpose of this Act is to protect New Zealand as a free, open, and democratic society by—
>
> (a) establishing intelligence and security agencies that will effectively contribute to—
>
> i. the protection of New Zealand's national security; and
>
> ii. the international relations and well-being of New Zealand; and
>
> iii. the economic well-being of New Zealand; …

In addition, s 9 of the ISA states that one of the "principal objectives" of the Agencies is "to contribute to the protection of national security"; and ss 58 and 60 permit the issuing of warrants to authorise otherwise unlawful activities that are necessary "to contribute to the protection of national security".

E.19. As contributing to the "protection of national security" is a purpose of the ISA, one of the Agencies' principal objectives and a basis for granting warrants authorising the Agencies' use of intrusive and otherwise unlawful powers, the term should, in principle, be defined. A definition would provide some constraint on the Agencies and guidance for those with oversight responsibilities under the ISA, as well as enhancing public understanding of the Agencies' work.

E.20. We recommend that a definition along the following lines be inserted in the interpretation section of the ISA, s 4:

> **protection of national security** means the protection of New Zealand, its communities and people from activities that are threats because they undermine, or seek to undermine, one or more of New Zealand's—
>
> (a) territorial integrity and safety, including the safety of its communities and people;
>
> (b) sovereignty, democratic institutions, processes, and values;
>
> (c) multi-cultural and diverse social fabric;
>
> (d) essential interests, including its critical infrastructure and governmental operations;
>
> and includes identifying and enabling the assessment of such threats.

E.21. A sentence along the following lines could be added to provide a non-exhaustive list of examples of the types of activity that would fall within the definition.

> Such activities include, but are not limited to, terrorism, espionage, sabotage, violent extremism, insurrection, foreign interference, cyberthreats, and serious transnational crime.

Other examples (such as money laundering) could be added, if deemed appropriate.

E.22. This definition does not seek to identify specific threats to national security; rather, it seeks to identify what it is about New Zealand that should be protected in the name of national security. This is because what national security seeks to protect remains relatively constant over time; what threatens national security changes with time – sometimes surprisingly quickly. Focusing on the former rather than the latter means the ISA can accommodate the changing threatscape without the need for legislative change.

E.23. This definition might be thought to be too general to place any real constraint on the Agencies, or to provide them with any real guidance about the scope of their work. We do not agree for the following reasons.

- By their nature, definitions of "national security" or "protection of national security" capable of accommodating changing threatscapes will have some inherent uncertainty. As it stands now, s 58 of the ISA, which states the current circumstances in which warrants for the protection of national security may be sought against New Zealanders, contains similar uncertainties, for example, in referring to "a New Zealand interest"[1] and "New Zealand's interests".[2]
- The definition would operate within a statutory context that provides a range of other controls that help with focusing the application of the definition.
  - The Agencies must collect and analyse intelligence "in accordance with the New Zealand Government's priorities".[3] If the envisaged priority setting is carried out effectively, that will constrain the Agencies' application of the definition.
  - Where the Agencies seek to use intrusive powers for "protection of national security" purposes, they will have to persuade both the Minister and a Commissioner of Intelligence Warrants that the circumstances make the issuing of such a warrant "necessary" and "proportionate". To make that determination, the Minister and the Commissioner will have to consider the objective of the warrant, and the activities it is intended to authorise, in the context of the definition.
  - The Inspector-General of Intelligence and Security (the Inspector-General) reviews all warrants for legality and propriety and may review activities the Agencies take under warrants. If the Inspector-General considers the issuing of a warrant, or any action taken under it, to be "irregular", they may report that to the relevant Minister and the Chief Commissioner of Intelligence Warrants. That again will require consideration of the link between the objectives of particular warrants and the definition.

E.24. Finally, we note that while we expect all threats-based warrants to be dealt with under the proposed definition, the Agencies would still have the power to seek warrants to carry out

---

1 Intelligence and Security Act 2017, s 58(2)(b)(i).

2 Section 58(2)(g)(i).

3 Section 10(1).

unlawful activities that "will contribute to" either New Zealand's international relations and well-being or New Zealand's economic well-being. These activities will be unaffected by the inclusion of the definition.

Removing the distinction between Type 1 and Type 2 warrants

E.25. The ISA draws a distinction between warrants applying to New Zealand citizens and permanent residents (New Zealanders) (referred to in the ISA as Type 1 warrants) and those applying to non-New Zealanders (Type 2 warrants). The requirements for issuing Type 1 warrants are more onerous than those for issuing Type 2 warrants. We consider the distinction between Type 1 and Type 2 warrants to be no longer necessary or meaningful and recommend it be abolished. The Agencies support this recommendation, and we heard no opposition to it from other parties we consulted.

E.26. The result would be that New Zealanders and non-New Zealanders would be treated alike in relation to warrants for the protection of national security, and non-New Zealanders would benefit from the higher standard presently applicable only to New Zealanders. Moreover, all such warrants would be issued by both the Minister and a Commissioner of Intelligence Warrants, acting together, so that both New Zealanders and non-New Zealanders would have the benefit of the so-called 'triple lock' mechanism.[4]

E.27. In respect of warrants to authorise activities that will contribute to New Zealand's international relations and well-being or to its economic well-being, we consider that the current differential requirements between New Zealanders and non-New Zealanders should remain. In essence, this type of warrant can only be granted against a New Zealander where there are reasonable grounds to suspect that the New Zealander is effectively a foreign agent.

E.28. We recommend removing the Type 1 / Type 2 distinction for the following reasons.

- It removes the current legal uncertainty as to when a Type 1 warrant must be obtained alongside a Type 2 warrant to cover the possible incidental collection of information concerning New Zealanders.
- As a matter of practice, it is now common for the Agencies to obtain 'partner' warrants – Type 1 and Type 2 warrants together. This means that the distinction between Type 1 and Type 2 warrants has little, if any, practical effect.
- New Zealanders are not, ultimately, disadvantaged in relation to warrants for the protection of national security. All that would happen is that non-New Zealanders would have the same level of protection as New Zealanders. From a human rights point of view, this would be the better approach.
- We are not recommending changes to the differentiation between New Zealanders and non-New Zealanders in relation to warrants for international relations or economic well-being. While the removal of the Type 1 / Type 2 distinction might alter the form of these authorisations, it would not enlarge the scope for targeting New Zealanders.

E.29. If this recommendation is accepted, there will be a number of consequential changes that will have to be made to the warranting regime. These are detailed in our report.

---

[4] This mechanism is referred to as the triple lock because it requires decisions by both the Minister and a Commissioner of Intelligence Warrants that a warrant should be issued, as well as a subsequent review by the Inspector-General.

Reforming Parliament's Intelligence and Security Committee

E.30. The Intelligence and Security Committee was established by the Intelligence and Security Committee Act 1996, following the establishment of the United Kingdom's Intelligence and Security Committee in 1994. While legislation governing the equivalent committees in Australia, Canada and the United Kingdom **prohibits** members of the Executive (such as the Prime Minister and other Ministers) from being members of the committee, the ISA **requires** that the New Zealand Committee be chaired by the Prime Minister. In addition, the New Zealand Committee will inevitably have among its members one or more additional Ministers, in particular, the Minister(s) responsible for the Agencies. Under the ISA, the Leader of the Opposition must also be a member, and there may be representatives of other parties.

E.31. Besides this difference in eligibility for committee membership, there are other ways the committees in Australia, Canada and the United Kingdom differ from the New Zealand Committee. They have jurisdiction over more agencies within the wider intelligence and national security community and may consider a broader range of matters. For example, both the Canadian and the United Kingdom committees have the power to consider operational issues and to exercise oversight of defence intelligence functions. The New Zealand Committee cannot do either.[5] Both publish substantive reports on the matters they consider, such as diversity in the intelligence and security agencies[6] and foreign interference in elections.[7] Also, the committees in all three countries are supported by a permanent secretariat, which is not the case for the New Zealand Committee.

E.32. The result is that, while there are differences between the various committees in Australia, Canada and the United Kingdom and they are subject to some control by the Executive, they have much greater capacity to exercise effective democratic oversight of the intelligence and security agencies in their countries than the committee does in New Zealand.

E.33. While the office of the Inspector-General was substantially strengthened in 2013 and the number of Commissioners of Intelligence Warrants was increased from one to three under the ISA, the Intelligence and Security Committee has remained essentially in the same form as it was when established in 1996, apart from the fact that it may now have between five and seven members (as opposed to the previous five). We recommend the Committee be substantially reformed so it can provide independent and effective democratic oversight of the Agencies, and that the reach of its oversight functions be extended.

E.34. To give a brief explanation of the reasons for this recommendation, we need to emphasise six features of the ISA.

- As we noted above, s 3(a) provides that the purpose of the ISA is to protect New Zealand as a free, open and democratic society by (among other things) establishing intelligence and security agencies that will effectively contribute to three sets of interests. There is, then, an expectation that the Agencies' contribution will be "effective".
- Section 3 also indicates that the ISA aims to ensure that the functions of the Agencies are performed "in a manner that facilitates effective democratic oversight"[8] and to ensure that

5 The Australian committee does not have the power to consider operational matters either.

6 Intelligence and Security Committee of Parliament *Women in the UK Intelligence Community (2015) and Diversity and Inclusion in the UK Intelligence Community* (2018).

7 United Kingdom, Intelligence Security Committee, *ISC Annual Report 2016–2017* (December 20, 2017).

8 Intelligence and Security Act 2017, s 3(c)(iii).

the Agencies powers are subject to "institutional oversight and appropriate safeguards". Section 17(d) imposes a duty on the Agencies to act in a manner that facilitates "effective democratic oversight".

- Part 6 of the ISA deals with oversight of the Agencies. Section 156(1) states that the purpose of the Part is "to provide for the independent oversight of intelligence and security agencies to ensure that those agencies act with propriety and operate lawfully and effectively".
- Under Part 6, the Inspector-General has three functions: to ensure that the Agencies act lawfully and with propriety, to ensure complaints are independently investigated and to advise the government and the Intelligence and Security Committee on matters relating to oversight of the Agencies.[9] The Inspector-General considers effectiveness only in relation to the Agencies' compliance with the ISA in terms of the issuing and execution of warrants and of the Agencies' compliance systems more generally.[10]
- In terms of Part 6, the main function of the Intelligence and Security Committee is to examine the Agencies' "policy, administration and expenditure".[11] The statutory provisions setting out the Committee's functions do not explicitly identify a function of assessing the Agencies' effectiveness, and there are other provisions that would make it hard to perform such a function, in particular, the prohibition on inquiring into any matter that is operationally sensitive (which includes matters relating to intelligence collection and production methods or sources of information).[12]
- Finally, we note that s 236(3) in Part 7 states that the terms of reference for periodic reviews, such as ours, "may include any matter relevant to the functions, effectiveness, and efficiency of [the Agencies] and their contribution to national security".

E.35. Four important points emerge from this brief overview. The ISA contemplates that:

- the Agencies will contribute **effectively** to the protection of national security and to the other two sets of interests
- there will be **effective democratic oversight** of the Agencies
- there will be **independent** oversight of the Agencies to ensure that they act **effectively**
- it is possible to assess the effectiveness of the Agencies and their contribution to national security.

E.36. We have concluded that the Intelligence and Security Committee should be the body providing 'independent' and 'effective democratic oversight' of the Agencies (including in relation to their effectiveness) under the ISA. We know from discussions with previous and present members of the Committee that it has not performed this function to date and, given its make-up and resources, it would be unreasonable to have expected it to do so. In its current form, the Committee cannot undertake the necessary oversight function.

9 Section 156(2).
10 Section 158(1)(f).
11 Section 193(1).
12 Section 193(2)(b).

E.37. As we see it, the Committee lacks:

- independence from the Executive
- the time and capacity to undertake meaningful scrutiny of the Agencies' work, in particular, in relation to their effectiveness
- the power to examine other agencies within the broader national security and intelligence community whose work raises similar issues to those raised by the Agencies' work and whose work is relevant to the Agencies' effectiveness.

E.38. Accordingly, we recommend the Committee be reformed. We will not summarise all the necessary changes here but note some of the more important ones as follows.

- Current members of the Executive should be prohibited from being members of the Committee.
- The Committee's membership should comprise Members of Parliament from significant parties represented in Parliament.
- The Committee's jurisdiction should be expanded so that it is able to:
  - investigate, consider and report on operational matters in relation to the Agencies, including methods of intelligence collection and production (with the possible exception of current operations)
  - exercise oversight of the principal intelligence assessment agency or agencies
  - exercise oversight of significant intelligence and national security functions performed by other government organisations or agencies, such as the NZDF and the Police.
- The Committee should be supported by a small secretariat (three or four people) of cleared staff.
- Committee members must be able to access the classified and confidential information necessary to enable them to perform their expanded mandate effectively.
- The ISA should make it clear that members of the Committee exercise their oversight functions on behalf of all New Zealanders rather than on a party-political basis.

E.39. We also suggest that consideration be given to empowering the Committee to consider the use by government departments and agencies of technologies involving the acquisition, aggregation, searching, analysis and manipulation of open-source and other data that results in biometric identifiers or other information of a sensitive personal nature.

E.40. The current demarcation between the work of the Committee and that of the Inspector-General would remain.

E.41. It will be important for the reformed Intelligence and Security Committee to be as open as reasonably possible about its work. Obviously, there will be significant limits on its ability to be transparent and much, perhaps most, of its work will necessarily be undertaken in secret. But it will be important for the Committee to demonstrate to New Zealanders that it is undertaking its expanded mandate rigorously on their behalf. Responding to relevant public concerns, issuing public reports, holding public hearings from time to time and similar measures will assist in this.

Other issues

E.42. There are several matters that we highlight as either areas of work in progress or areas that need further examination.

Recognising New Zealand's diverse and multi-cultural society

E.43. In our proposed definition of "protection of national security", we have highlighted New Zealand's increasingly multi-cultural and diverse society as one of the country's features that requires recognition in a national security context. The 2018 Census identified six major ethnic groups in New Zealand – European (70.2%); Māori (16.5%); Pacific peoples (8.1%); Asian (15.1%); Middle Eastern / Latin American / African (1.5%); and other ethnicity (1.2%). Within those major groups, there are many other communities – as at 2018, there were over 160 ethnic groups containing more than 100 people living in New Zealand.

E.44. The Agencies have worked in recent years to increase the diversity of their workforce, as well as their outlook and practices. While these efforts are commendable, our consultations and observations indicate that there is still much to be done to achieve true diversity and inclusion within the Agencies, and within the national security system more generally. We therefore recommend that s 3 of the ISA be amended to include a reference to the Crown's obligations to Māori under te Tiriti o Waitangi / the Treaty of Waitangi and the need for the Agencies to perform their functions in a manner that reflects New Zealand's multi-cultural and diverse society. Corresponding changes should also be made to s 17, which sets out the general duties of the Agencies when performing their functions.

Developing a coherent and consistent policy and legislative framework for New Zealand's national security system

E.45. Although this review was never intended to be a 'root and branch' review, we have identified some issues of a fundamental structural nature that we think should be addressed at some point. Perhaps the most important of these is the lack of a coherent legislative framework governing the overall intelligence and security community. Like the Royal Commission, we feel there are governance and accountability gaps and legislative inconsistencies and incoherence. In an area as important as national security, where numerous agencies have the capacity to make meaningful contributions, and in circumstances where technological tools are developing so quicky, there needs to be a comprehensive and coherent policy and legislative approach across the sector.

Working from a 'need to share' rather than 'need to know'

E.46. A coherent and coordinated national intelligence and security system is also based on effective cooperation and information sharing between domestic agencies, which facilitates a joined-up approach to responding to national security threats. Intelligence is only valuable where it leads to something, whether better decision-making, improved public safety or addressing threats to national security. As the Royal Commission noted,[13] previous reviews of components of the national security system have emphasised the need to ensure the right information gets to the right people at the right time so that it can be used effectively.

[13] Royal Commission of Inquiry *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) at part 8, chapter 9 [9]–[13].

E.47. We believe the ISA is generally enabling in terms of information sharing, rather than a hinderance. Despite that, there are still barriers to information sharing domestically. These are mostly institutional or cultural barriers or barriers associated with technology and infrastructure. One of the points that emerged in our consultations was concern over an approach to classified information that emphasises the 'need to know'. In other words, to receive such intelligence, a person must hold an appropriate security clearance and must need to know the particular information in order to perform their duties. This approach places a high value on maintaining secrecy to avoid compromising intelligence sources and methods and requires the holder of information to determine who needs to know about that information.

E.48. We prefer a different approach. We consider that a greater emphasis should be placed on the 'need to share' information to ensure that the full value of the Agencies' intelligence-gathering and assessment activities is realised. The 'need to share' involves a different mindset than the 'need to know' and applies not just to the Agencies but across the national security and intelligence system. We acknowledge there is a balance to be struck between sharing intelligence more widely and the potential for compromise and prejudice to New Zealand's interests. However, a greater government-wide appreciation of the national security benefits of information sharing may prove beneficial in the longer term.

Changing the focus of regulatory efforts

E.49. We have referred to the paradigm shift in technological developments and the impact on intelligence and security agencies. Given the proliferation of commercially and publicly available data, it may be that, in the longer term, regulatory efforts will have to focus as much on the use by intelligence and security agencies (and other state agencies) of open-source data as they currently do on the agencies' use of intrusive powers to obtain data.

E.50. To give an example from overseas, a private-sector company, which has access to a near real-time database of billions of geolocation signals from mobile phones, sells a subscription service to law enforcement agencies. This enables the agencies to obtain mobile phone location data for particular locations of interest or particular devices of interest in near real-time. The company acquires the data from third-party applications on mobile phones, which have permission to collect users' location data. The app owners sell that information to third-party advertisers or data processors. The data may then be on-sold and amalgamated, to form databases of the type just described.

E.51. This type of commercial activity has profound implications for law enforcement and other state agencies, for mobile phone users and for society more generally. There will be a time when New Zealand will need to address the issues that this type of commercial activity raises. This challenge may well require changes in regulatory focus in future.

Threat disruption

E.52. The paradigm shift in technological developments has another effect in that malicious actors are increasingly using such developments to threaten and cause harm to New Zealand's national security interests. One issue raised during our review was whether the Agencies should have more extensive threat disruption powers, given they are, with limited exceptions, not enforcement agencies.

E.53. Currently, the GCSB is entitled under the ISA to do everything that is necessary or desirable to protect the security and integrity of communications and information infrastructures of

importance to the government as an exception to the enforcement prohibition. This disruption activity is reactive in nature, in the sense that it responds to threats. Moreover, the GCSB is not permitted to undertake disruption activities in other contexts, such as counterterrorism.

E.54. In the case of the NZSIS, the Inspector-General has accepted that the NZSIS is entitled to give warnings in certain contexts without infringing the prohibition on undertaking enforcement activities. We have recommended that this be clarified.

E.55. We have given thought to the larger question of whether the Agencies should be given wider powers of threat disruption. While we consider there is a case for allowing the Agencies to undertake more threat-disruption work, the issue is complex and raises significant policy questions that need thorough examination. We have recommended that this policy work be undertaken as a priority.

Other matters

E.56. We have also considered a range of other matters as part of our review and in accordance with our terms of reference. These are detailed further in our report. In the main, they respond to concerns with the operation of the ISA raised by the Agencies, the Inspector-General or domestic agencies. Adequately responding to these has necessarily required some detail on highly technical matters. Our specific recommendations on these matters are outlined in the report. They are also set out in the summary of recommendations chapter, which we drafted so that it could also be read as a stand-alone document.

SECTION 01

Some background

CHAPTER 01
Setting for the review

Introduction

1.1. In this chapter, we give the background to our review.

- First, we describe the origins of the statutory requirement for the review and refer briefly to the earlier review carried out by Sir Michael Cullen and Dame Patsy Reddy (the Cullen/Reddy review).[14]
- After that, we introduce the Intelligence and Security Act 2017 (ISA), which resulted from the Cullen/Reddy review.
- Then we outline the purpose and nature of our review.
- Next, we give a brief history to the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019 (the Royal Commission), which made recommendations relevant to our review.
- We then identify the various work streams underway as part of the government's response to the Royal Commission recommendations.
- Finally, we describe the approach we have taken in our review.

Cullen/Reddy review

1.2. In 2013, a group of sections was inserted into the Intelligence and Security Committee Act 1996 to provide for periodic reviews of the two intelligence and security agencies (the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) and referred to in our report as 'the Agencies') and their associated legislation. At that time, there were four relevant Acts – one for each Agency[15] and one each for the Inspector-General of Intelligence and Security[16] and the Intelligence and Security Committee[17]. This resulted in legislative inconsistency and lack of coherence. In addition to the legislative hodgepodge, there had been ongoing public controversies surrounding various of the Agencies'

---

[14] Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM *Intelligence and Security in a Free Society – Report of the First Independent Review of Intelligence and Security in New Zealand* (February 2016) (*Cullen/Reddy report*).

[15] Government Communications Security Bureau Act 2003 and New Zealand Security Intelligence Service Act 1969 respectively.

[16] Inspector-General of Intelligence and Security Act 1996.

[17] Intelligence and Security Committee Act 1996.

activities, notably in relation to the GCSB's surveillance of Mr Kim Dotcom in support of New Zealand Police (the Police).[18]

1.3. The Government Communications Security Bureau and Related Legislation Amendment Bill (the Amendment Bill) was introduced into Parliament against this background in May 2013. It was intended to improve various features of the existing legislation. The periodic review provisions were introduced into the Amendment Bill by means of a Supplementary Order Paper introduced by Hon Peter Dunne after the Amendment Bill had emerged from the Intelligence and Security Committee. Under the legislation as ultimately enacted, a review could consider "any matter relevant to the functions, effectiveness, and efficiency of the intelligence and security agencies and their contribution to national security".[19]

1.4. Sir Michael Cullen and Dame Patsy Reddy undertook the first statutory review in 2015. The terms of reference described the purpose of their review as being to determine:

- whether the legislative frameworks of the Agencies were well placed to protect Aotearoa New Zealand's current and future national security, while protecting individual rights
- whether the current oversight arrangements provided sufficient safeguards at an operational, judicial and political level to ensure that the Agencies acted lawfully and maintained public confidence.

1.5. The terms of reference for the Cullen/Reddy review related to the two Agencies and their oversight arrangements. In the publicly available Cullen/Reddy report, there is also some discussion of the National Assessments Bureau (NAB), which was (and remains) located in the Department of the Prime Minister and Cabinet (DPMC) and provides intelligence assessments.[20]

1.6. The Cullen/Reddy report highlighted the need for intelligence priorities and for greater coordination between the two Agencies and the NAB and, to that end, recommended the establishment of a National Intelligence and Security Adviser to oversee and coordinate the three entities. It also highlighted the need for greater cooperation and sharing of information with other agencies, such as the New Zealand Defence Force (NZDF) and the Police.[21] But the broader intelligence community, and the structures governing it, was not a focus of the Cullen/Reddy review.

1.7. This is significant because there are other government entities than the GCSB, the NZSIS and the NAB that perform intelligence and security functions. The two most obvious examples are the NZDF and the Police. Other government departments also have intelligence and assessment capabilities, for example, the Ministry of Business, Innovation and Employment (MBIE), the New Zealand Customs Service (Customs), the Ministry for Primary Industries (MPI) and, more recently, the Department of Internal Affairs (DIA).

---

[18] For a description of the different controversies, see, for example, Damien Rogers and Shaun Mawdsley "Restoring Public Trust and Confidence in New Zealand's Intelligence and Security Agencies: is a parliamentary commission for security the missing key?" (February 2022) 18(1) *Policy Quarterly 59* and Alister Gillespie and Claire Breen "The Security Intelligence Agencies in New Zealand: evolution, challenges and progress" (2021) 36(5) *Intelligence and National Security 676*.

[19] Intelligence and Security Committee Act 1996, s 22(3)(a).

[20] The Combined Threat Assessments Group (CTAG) located within the NZSIS also undertakes threat assessments. At para [4.34], the Cullen/Reddy report said: "we recommend the government should review the current placement of CTAG within NZSIS and consider whether it might more appropriately be situated with the NAB".

[21] Cullen/Reddy report, at recommendation 31.

1.8. In addition, the GCSB, the NZSIS and the NAB ultimately depend on the various agencies that sit on the government's Security and Intelligence Board[22] to be effective in helping protect New Zealand's national security. This includes, for example, understanding what they should prioritise and what is required and taking action on the intelligence and assessments they produce. As we discuss later in this report, simply focusing on the GCSB and the NZSIS and their accountability and review arrangements is arguably too narrow a perspective when assessing the effectiveness of the national security system. There needs to be a broader approach – such as, for example, ensuring a greater degree of integration or complementarity between the legislation governing the GCSB and the NZSIS and that governing other organisations within the national security and intelligence community, such as the NZDF.

1.9. The Cullen/Reddy report was published on 29 February 2016. An important recommendation was that the four existing statutes be repealed and replaced by a single Act.[23] This led ultimately to the enactment of the Intelligence and Security Act (ISA), which was passed on a substantially multi-party basis.[24]

1.10. Section 235 of the ISA requires a review of the Agencies and of the ISA every 5 to 7 years. As with the repealed review provisions, under s 235 of the ISA, the terms of reference for a review may include "any matter relevant to the functions, effectiveness, and efficiency of the intelligence and security agencies and their contribution to national security". When originally enacted, the effect of s 235(a) of the ISA was that the first review would commence towards the end of 2022. However, after the Royal Commission reported in November 2020, s 235(a) was amended to provide that the first review would take place as soon as practicable on or after 1 July 2021. This reflected the fact that the Royal Commission had made several recommendations relevant to the review that needed to be considered on an accelerated timeframe.

The Intelligence and Security Act 2017

1.11. We will discuss the detail of the ISA at relevant points in the chapters that follow. For present purposes, it is sufficient to refer to the ISA's purpose. That is described in s 3 as:

> **Purpose**
>
> The purpose of this Act is to protect New Zealand as a free, open, and democratic society by—
>
> (a) establishing intelligence and security agencies that will effectively contribute to—
>
> (i) the protection of New Zealand's national security; and
>
> (ii) the international relations and well-being of New Zealand; and
>
> (iii) the economic well-being of New Zealand; and

[22] DPMC, MFAT, Customs, MBIE, Police, NZDF, and the Ministry of Defence.

[23] There were, of course, other important recommendations, some of which we will refer to in subsequent chapters.

[24] The debates are notable for the bipartisan spirit in which they were conducted. During the third reading debate, Hon Andrew Little, then Leader of the Opposition, acknowledged the efforts of the Attorney-General, Hon Christopher Finlayson KC, to ensure a bipartisan approach to the legislation: "I rise to support the bill at its third reading and to acknowledge the work of the Minister, Christopher Finlayson, who has just spoken, for doing the spadework and also the effort that he has put in, in dealing with other parties, listening to their concerns openly and genuinely, and seeking to resolve the outstanding matters that each of the parties had brought to him."((21 March 2017) 721 NZPD (Intelligence and Security Bill – Third Reading, Hon Andrew Little)). The Bill passed its third reading with only the members of the Green Party voting against it.

> (b) giving the intelligence and security agencies adequate and appropriate functions, powers, and duties; and
>
> (c) ensuring that the functions of the intelligence and security agencies are performed—
>
> (i) in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; and
>
> (ii) with integrity and professionalism; and
>
> (iii) in a manner that facilitates effective democratic oversight; and
>
> (d) ensuring that the powers of the intelligence and security agencies are subject to institutional oversight and appropriate safeguards.

1.12. There are six features of this section worth emphasising here as they are significant for the issues in our review.

The democratic paradox

1.13. First, s 3 identifies the ISA's fundamental purpose as being "to protect New Zealand as a free, open, and democratic society". There is, however, a paradox inherent in national security measures in liberal democratic societies. Some measures are necessary to protect a democracy's institutions, its governmental structures and processes and the physical safety, rights and freedoms of its people from attack or subversion by malicious actors. However, those measures can involve some interference with the rights and freedoms of those being protected, the extent of which may well be controversial. As it has been put recently:[25]

> We fear the perfidious actions of 'others'; so, we create or expand security and intelligence institutions to protect us, but then we fear the very institution we have created for protection.

We will return to the democratic paradox in later chapters of our report.

The Agencies' contribution

1.14. Second, s 3(a) contemplates that, in fulfilling the ISA's fundamental purpose, the Agencies will contribute to three sets of interests: first, the protection of New Zealand's national security; second, New Zealand's international relations and well-being and third, its economic well-being. Section 9 gives effect to this by stating that the "principal objectives of the intelligence and security agencies are to contribute to [the three sets of interests.]" This description is based on the statement of the GCSB's objective in s 7 of the Government Communications Security Bureau Act 2003, as amended in 2013.

1.15. We make three observations about this.

- The scope of the Agencies' activities is potentially very broad. The breadth of the language in s 3(a)(i)–(iii) indicates this. In many situations, however, New Zealand's international relations and well-being, economic well-being and national security are inextricably linked, or at least have a significant degree of overlap.

[25] Christian Leuprecht and Hayley McNorton *Intelligence as Democratic Statecraft* (2021, OUP) at 1.

- The term "national security" is not defined in the ISA, although the Cullen/Reddy report recommended a definition and the Bill, as introduced, contained one. The select committee that considered the Bill (the Foreign Affairs, Defence and Trade Committee) recommended the definition be removed, and that recommendation was accepted. We will return to the issue of definition of "national security" in chapter 5. We simply note at this point that because the government has for many years taken an 'all hazards, all risks' approach to national security, the concept can be very broad.[26] Similarly, the reference to New Zealand's well-being in s 3(a)(ii) is open ended.
- The breadth of the language of s 3(a)(i)–(iii) means that there must be other mechanisms to focus and control the Agencies' actions. The ISA does contain processes that are intended to narrow the operational focus of the Agencies, in particular, priority setting mechanisms, limitations on the circumstances in which intrusive powers can be exercised and oversight and accountability mechanisms. We will explain these processes and comment on their effectiveness later in this report.[27] Here, it is sufficient to note that it is important not to consider issues in isolation but, rather, to assess them in their broader context. In other words, the ISA has to be viewed as a whole rather than through the lens of one or other aspect of it.

Effectiveness

1.16. Third, s 3(a) contemplates that the Agencies' contribution to the three sets of interests will be "effective". This is relevant to our consideration of:

- the Agencies' powers (ie, do they enable the Agencies to be effective in contributing to the identified sets of interests?)
- the ISA's accountability mechanisms (ie, do they provide for appropriate assessment or evaluation of the Agencies' effectiveness?).

1.17. Underlying these issues is the difficult question of how the 'effectiveness' of an intelligence and security agency, or a particular power available to an agency, is to be assessed and by whom. We return to this topic in chapters 4 and 12 but note the Royal Commission's conclusion that:[28]

> … there is still no performance framework in place to measure the efficiency and effectiveness of New Zealand's intelligence community or counter-terrorism effort, or their delivery against the National Security and Intelligence Priorities.

"Appropriate" powers

1.18. Fourth, s 3(b) refers to giving the Agencies functions, powers and duties that are "adequate and appropriate". It is not one of the Agencies' functions to enforce measures for national security (apart from certain limited exceptions),[29] a point to which we return in chapters 5 and 10. The word 'adequate', read in context, must relate back to the effective contribution that the ISA

---

[26] The government has consulted on its first national security strategy based on a narrower concept of national security: "protecting New Zealand from threats from those who would do us harm." DPMC "National Security Backgrounder: Aotearoa New Zealand's First National Security Strategy" (12 August 2022); DPMC Aotearoa's National Security Strategy (dpmc.govt.nz/our-programmes/national-security/aotearoas-national-security-strategy).

[27] See chapter 4 for a general overview and chapter 12 for a more detailed discussion.

[28] Royal Commission of Inquiry *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) at part 8, chapter 3 [79] (Royal Commission report).

[29] Intelligence and Security Act 2017, s 16.

contemplates the Agencies will make to the three sets of interests. So, the Agencies must have sufficient powers to enable them to achieve that outcome (against the background that they are generally prohibited from carrying out enforcement measures).[30]

1.19. In context, the word 'appropriate' seems to introduce an evaluative component. For example, there may be powers that would help the Agencies make an effective contribution to the sets of interests (thus meeting the adequacy test) but that would be seen as inappropriate for some reason (overreach, for example). This evaluative element is consistent with the obligation the ISA imposes on the Inspector-General of Intelligence and Security to consider both the legality and propriety of the Agencies' actions.[31]

The Agencies' obligations

1.20. Fifth, s 3(c) deals with the Agencies' obligations in performing their functions. In terms of s 3(c)(i)–(iii), the ISA is intended to protect New Zealand as a free, open and democratic society by ensuring that the Agencies' functions are performed lawfully and consistently with human rights obligations recognised by New Zealand law, with integrity and professionalism and in a way that facilitates democratic oversight. Section 17 of the ISA requires the Agencies to meet the standards identified in s 3(c)(i)–(iii) but adds one further standard, namely that, when performing their operational functions, the Agencies must act "independently and impartially". It is not clear why this additional standard was not included in s 3(c).

1.21. Further, the Directors-General of the Agencies have a duty under s 18(a)(iii) to take all reasonable steps to ensure that the Agencies' activities are "politically neutral". It is not obvious how this adds anything to the Agencies' duty to act "independently and impartially". But if it is seen as adding something, or as serving an important symbolic function, it is not clear why it is not also identified in s 3(c), given that it is a fundamental obligation in a democratic society. Nor, finally, is it clear why there is no reference to the Agencies being required to act consistently with te Tiriti o Waitangi / the Treaty of Waitangi (te Tiriti o Waitangi) in s 3(c) or s 17.

1.22. We will discuss these matters further in this report.

Oversight and safeguards

1.23. Finally, s 3(d) emphasises the important point that part of keeping New Zealand as a free, open and democratic society is ensuring that the Agencies' powers are subject to "institutional oversight and appropriate safeguards". Here 'appropriate' simply means 'suitable'.

1.24. The ISA attempts, in a variety of ways, to implement the elements of s 3. In the chapters that follow, we will consider how effectively it does so in particular contexts.

---

[30] GCSB is an enforcement agency under the Telecommunications (Interception Capability and Security) Act 2013 for network security purposes (part 4, subpart 7).

[31] Intelligence and Security Act 2017, s 156(2)(a)(i) (discussed further in chapter 12).

The purpose of our review

1.25. The terms of reference[32] make it clear that our review is not intended to be a fundamental reappraisal of the legislative framework established by the ISA, ie, it is not a 'root and branch' review. The preamble to the terms of reference states:

> The Cullen-Reddy review was a fundamental review that resulted in substantial changes to the legislative framework. The 2021 review is not intended to replicate the scope of the 2016 review, or to be a first principles review of the Act. The intent of this review is to understand what improvements need to be made, if any, so that the Act is clear, effective, and fit for purpose, as well as considering matters raised by the [Royal Commission] report.

1.26. Under the terms of reference, our review has the two purposes of:

- determining whether improvements could be made to the ISA "to ensure it continues to be effective, clear and fit for purpose"
- considering the recommendations and issues related to the ISA that were raised in the Royal Commission's report.

1.27. In conducting our review, we were directed to "have particular regard to" certain matters, specifically:

- whether the ISA appropriately balances national, community and individual security with individual privacy and other rights
- whether the ISA sufficiently enables and controls target discovery activity by the Agencies
- whether the authorisation framework under the ISA can be improved to better serve the purpose of the ISA
- whether the ISA adequately provides, and has appropriate protections and oversight in place, for both Agencies to collect intelligence (in particular, the processing, analysis, retention and destruction of collected information/data)
- how the ISA may best enable the Agencies to appropriately and effectively cooperate and share information with New Zealand government agencies and other partners
- any other matters that arise during the course of the review, as agreed by the Prime Minister and notified in writing in the *New Zealand Gazette*.

No other matters have been designated in terms of paragraph [1.27] above.

1.28. We note that the purpose of our review is to assess the ISA, not the Agencies or other entities that operate under the ISA. As such, we make various recommendations that we consider will improve the ISA. Some reflect existing practices but are matters that we consider the ISA should address explicitly; others would change practices.

1.29. Recommendations for change to the ISA do not necessarily imply criticism of the Agencies or the other entities that operate under the ISA.

---

[32] The terms of reference are provided in appendix A of this report.

The Royal Commission and its recommendations

1.30. The Royal Commission was established on 8 April 2019 following the terrorist attack on Al-Noor and Linwood mosques in Christchurch on 15 March 2019 to investigate the circumstances around those events. The investigation was conducted by Hon Sir William Young KNZM as Chair and Ms Jacqui Caine as Commissioner. The Royal Commission's work was completed on 26 November 2020, when it provided its final report to the Governor-General of New Zealand, Dame Patsy Reddy.

1.31. In its terms of reference, the Royal Commission was directed to examine four aspects:

- what relevant State sector agencies knew about the activities of the terrorist in relation to the attacks before they occurred
- what actions (if any) relevant State sector agencies took in light of that knowledge
- whether there were any additional measures that relevant State sector agencies could have taken to prevent the attacks
- what additional measures should be taken by relevant State sector agencies to prevent such terrorist attacks in the future.

1.32. The Royal Commission made 44 recommendations, 18 of which concern New Zealand's counter-terrorism effort. Its specific recommendations relating to the ISA are found within its broader suite of interlinked recommendations for a more cohesive and strategic counter-terrorism (and, by extension, national security) system.

1.33. The Royal Commission's core recommendation to achieve this is through:[33]

> … a new national intelligence and security agency that is well-resourced and legislatively mandated to be responsible for strategic intelligence and security leadership functions including a chief executive who is designated as the intelligence and security adviser to the prime minister and to cabinet … and operating as the sector lead and co-ordinator for strategic intelligence and security issues.

1.34. This agency would take over some of the work currently done within DPMC and would be accountable to a minister with sector-wide responsibility to lead the counter-terrorism effort.[34]

1.35. There are four recommendations that relate directly to the ISA.

- recommendation 6: Strengthen the role of the Intelligence and Security Committee
- recommendation 10: Add a reporting requirement to the ISA for direct access agreements
- recommendation 17: Require the National Intelligence and Security Priorities and the annual threatscape report to be published and considered by the Intelligence and Security Committee
- recommendation 18: Review all counter-terrorism legislation, including an urgent review of the effect of s 19 of the ISA on target discovery.

---

33 Royal Commission report, at recommendation 2.

34 Royal Commission report, at recommendation 1.

1.36. We will consider these recommendations at appropriate points in later chapters. We will also consider several other suggestions and observations made by the Royal Commission about matters relevant to our review at appropriate points.

The government's response to the Royal Commission recommendations

1.37. On 8 December 2020, the Prime Minister Rt Hon Jacinda Ardern announced that the government accepted and agreed in principle to implement all the recommendations contained in the Royal Commission's report.[35] On 7 December 2020, Hon Andrew Little (the Minister Responsible for the GCSB and the NZSIS) was appointed Lead Coordination Minister for the government's response to the Royal Commissions report, in accordance with the Royal Commission's recommendation 43. DPMC was assigned responsibility for coordinating the all-of-government response to the Royal Commission report.

1.38. In announcing its response to the Royal Commission, the government made a commitment "to work with community and interest groups across New Zealand". On 12 June 2021, Hon Andrew Little announced the establishment of the Ministerial Advisory Group on the government's Response (recommendation 44 of the Royal Commission report). The group – Kāpuia – comprises 30 people from diverse backgrounds and across New Zealand, including representation from affected whānau, survivors and witnesses, representative communities, civil society, local government and the private sector. As we discuss further below, we took the opportunity to engage with Kāpuia during our review, as well as with individual community representatives and groups.

1.39. Of particular relevance to our review was the government's response to the Royal Commission recommendations 1–11 and 17 related to changes to the national security machinery. The government is:[36]

> … reforming the national security sector including the structure of national security agencies, monitoring and governance structures and information sharing practices, as well as taking a more strategic approach to national security and engaging with the public on national security risks.

1.40. Our terms of reference direct us to be cognisant of the government's work in this area as it develops, while clarifying that the Royal Commission recommendations on machinery of government will be addressed as part of DPMC's policy work programme.[37]

1.41. The government has also made announcements related to work on other recommendations made by the Royal Commission on countering terrorism and violent extremism, social cohesion, reducing hate crimes and racism, and firearms safety. These include the following.

---

35 Cabinet Paper "Government Response to the Royal Commission of Inquiry into the Terrorist Attack on Christchurch Masjidain" (8 December 2020) CAB-20-SUB-0516.

36 Department of the Prime Minister and Cabinet "Royal Commission of Inquiry Response Progress Tracker" (July 2022) Department of the Prime Minister and Cabinet website <Response Progress | Department of the Prime Minister and Cabinet (DPMC)>.

37 "2022 Review of Intelligence and Security Act" (2 March 2022) *s* at [3.6].

- In relation to Royal Commission recommendations 4, 7, 8, 12–16 and 18, the government's work includes introducing the Counter-Terrorism Legislation Bill to amend various provisions in the Terrorism Suppression Act 2002, the Search and Surveillance Act 2012 and the Terrorism Suppression (Control Orders) Act 2019. The Bill was enacted with broad support and received Royal Assent in October 2021. On 19 October 2022, the government announced its intention to introduce further amendments to the Terrorism Suppression (Control Orders) Act to strengthen it. In June 2022, He Whenua Taurikura, National Centre of Research Excellence for Preventing and Countering Violent Extremism, was opened, bringing together academia, civil society and government to produce research specific to New Zealand.
- In relation to Royal Commission recommendations 25–38, the government's work has included the establishment of the Ministry for Ethnic Communities on 1 July 2021 to strengthen the government's work on social cohesion. In addition, the Ethnic Communities Graduate Programme in the public service was created. A social cohesion framework for the government and the education sector has been developed, including a $2m fund for community social cohesion initiatives.[38]
- In relation to Royal Commission recommendations 39–42, the government committed to introducing legislation on hate speech in 2022.[39] The Police's Te Raranga programme became fully operational in 2020. This programme aims to drive improvements in frontline Police practice to identify, record and manage hate crime and deliver a service that is more responsive to victims. The DIA has extended the Safer Communities Fund to enable communities at risk of hate crime and terrorism to upgrade their security arrangements.
- In relation to Royal Commission recommendations 19–24, the government has also been implementing systemic changes related to firearms, including new regulations for firearms applicants who have lived overseas.

Our approach

1.42. As mentioned, our review was not intended to be a 'root and branch' review. Rather, it was intended to identify any improvements that could be made to the ISA "to ensure that it continues to be effective, clear, and fit for purpose" and to consider relevant matters raised in the Royal Commission's report.

1.43. While operating within that framework, we have identified some issues of a fundamental structural nature, which we will raise so that others can consider them as appropriate. The most significant example is the legislative framework (or lack of it) applying to the overall intelligence and security system. At present, there are governance and accountability gaps, inconsistencies and incoherence at a legislative level.

[38] Ministry of Social Development *Social Cohesion Framework* (online, 2022).

[39] The government has introduced the Human Rights (Incitement on Ground of Religious Belief) Amendment Bill. During its first reading Kiritapu Allan noted that the Law Commission is set to carry out a comprehensive review of incitement, discrimination, and hate crime laws. Refer to Kiritapu Allan's First Reading speech for the Human Rights (Incitement on Ground of Religious Belief) Amendment Bill (13 December 2022).

1.44. In addition, some of the particular matters which our terms of reference directed us to raise points of fundamental importance, in particular, the appropriate balance between security interests and individual rights, which was a theme of the Royal Commission's report. They go to the essence of the ISA.

1.45. Our terms of reference required us to consider certain matters when conducting our review. They are:

- the principles agreed by Cabinet to guide the response to the Royal Commission
- that the Review should be underpinned by te Tiriti o Waitangi and its principles
- that the Review should enhance trust and confidence in the Agencies
- the need for the law to provide clear and understandable parameters of operation
- that the establishment of a new national intelligence and security agency (recommendation 2 of the Royal Commission) was being considered by DPMC as part of a review of the overarching national security policy settings and we would need to be cognisant of that work as it developed
- that the structure and current separation of the Agencies would be considered as part of DPMC's work on the overarching national security policy settings.

Further, we were required to meet communities' expectations of transparency as far as possible and give a wide range of members of the public the opportunity to express their views.

1.46. Broadly speaking, our work has involved four elements.

1.47. First, we attempted to understand the intent of the ISA from the legislation itself, from the debates as the legislation went through the House (including in select committee), from the work of officials supporting the parliamentary process and from the Cullen/Reddy report. The ISA had multi-party support – after a full debate, it was passed by a vote of 106 to 14, with the nays being Members representing the Green Party. Even though the Greens opposed the Bill, they did not dispute that intelligence and security agencies were, in principle, necessary. Rather, they were concerned about the extent of the powers being given to the Agencies and the nature of New Zealand's involvement with overseas partners.

1.48. We have found the parliamentary debates helpful in understanding what it was hoped the ISA would achieve, especially the speeches of the Minister responsible for the conduct of the Bill through the House, Hon Chris Finlayson KC, and of Hon Andrew Little as Leader of the Opposition. Several areas of contention arose in the debates, which were resolved by acknowledging they could be revisited in the first periodic review. An example is the size and composition of the Intelligence and Security Committee.[40] We will address these issues in further chapters of this report. At this point, we simply note that the insights we obtained from the debates and other Parliamentary material gave us gave us a baseline from which to work.

1.49. Second, we examined how the ISA operates in practice and the perceived problems with it. There were several elements to this.

[40] Refer to Andrew Little's (then Leader of the Opposition) Third Reading speech for the Intelligence and Security Bill (21 March 2017) 721 NZPD (Intelligence and Security Bill – Third Reading, Hon Andrew Little).

- We had to gain an understanding of what the core national security and intelligence agencies do and how they do it. Accordingly, we received numerous briefings from the Agencies and visited several of their facilities, observed their work and engaged with their personnel. We received written submissions from them on aspects of the ISA's provisions, as we will outline in later chapters. We also met twice with the NAB and received assessment reports to understand its function.
- We met with the DPMC, given its role in administering the ISA, and sought to understand the leadership and coordination of the national security system, including meeting with the deputy chief executive of the National Security Group and the National Security Policy Directorate as well as receiving briefings from the National Intelligence and Risk Coordination Directorate, which coordinates intelligence priorities guiding the Agencies and the NAB, the Royal Commission of Inquiry Response Group, and DPMC's strategic coordinators. DPMC also provided helpful written material.
- We needed also to understand how the various oversight mechanisms provided for in the ISA operate. We therefore engaged with the Inspector-General of Intelligence and Security (and his Deputy) and received written submissions from him on aspects of the ISA's operation. We also engaged with his predecessor and her Deputies. We had discussions as well with the Chief Commissioner of Intelligence Warrants and other Commissioners and with past and present members of the Intelligence and Security Committee. We needed to understand how they perceived their roles under the ISA and whether they had any views on the ISA's functioning, either as it affected their roles or more generally. We also met with the Auditor-General to understand his broad role and powers as auditor of the Agencies.
- We invited submissions from, spoke to and hosted workshops with other government agencies that interact with the Agencies, including the NZDF, the Police, Customs, MBIE, the Ministry of Foreign Affairs and Trade (MFAT), the Department of Corrections, MPI, Inland Revenue, the Serious Fraud Office, the Overseas Investment Office, Oranga Tamariki and Waka Kōtahi / New Zealand Transport Agency.
- We also invited submissions from and/or interviewed public officials who have an interest in the Agencies because of the roles they perform, such as the Chief Ombudsman, the Privacy Commissioner, the Chief Commissioner of Human Rights and the Independent Police Conduct Authority. Again, our purpose was to gain an understanding of how the ISA operates from the varied perspectives of these important office holders.
- We contacted and invited submissions from a wide range of non-governmental organisations, for example, professional organisations such as the New Zealand Law Society and Te Hunga Rōia Māori o Aotearoa (The Māori Law Society); faith-based organisations such as The Federation of Islamic Associations of New Zealand, Islamic Women's Council New Zealand and the New Zealand Jewish Council, as well as the New Zealand Chinese Association, representing New Zealand's largest ethnic community after Pākehā, Māori and Pacific peoples. We also invited submissions from telecommunications network operators and financial service providers, which have particular obligations under the ISA. We held a hui with representatives of the National Iwi Chairs Forum, which was valuable in informing our understanding of the issues from a Māori perspective. Importantly, given the recommendations in the Royal Commission's report, we engaged with Kāpuia on three occasions, both in person and remotely, and received helpful comments and feedback from the group, which are reflected at various points in the following chapters.

- We also contacted academics with research interests in intelligence and security. We held a day-long roundtable with some to discuss issues around oversight of the Agencies and sought feedback from them on some initial proposals in our review.
- Finally, we sought to engage the public on issues about the ISA. This accorded with the direction in our terms of reference that we would "need to meet communities' expectations of transparency as far as possible, and a wide range of members of the public should have the opportunity to express their views on the issues relating to the review". It also reflected the Royal Commission recommendations that more should be done to promote public understanding and discussion of national security issues. To that end, we provided the opportunity for the public to participate in a survey and to provide submissions; we reviewed public commentary and attended He Whenua Taurikura Hui, the National Hui on Countering Terrorism and Violent Extremism, held in Auckland on 30 October–1 November 2022.

1.50. Third, we undertook our own research by examining what occurs in jurisdictions such as Australia, Canada, the United Kingdom and the United States of America (the United States) and spoke to people performing oversight roles in all those jurisdictions except the United States. We also examined some of the academic and other literature that has been produced over the last few years, especially following the Snowden revelations in 2013,[41] including the extensive work carried out in the European Union.

1.51. Fourth, we tested our preliminary ideas for changes that were likely to be viewed as significant with those who might be affected and others consulted in the information-gathering stage before we reached the concluded views expressed in this report.

1.52. Finally, in writing our report, we were conscious of:

- the Royal Commission recommendations concerning greater public engagement and discourse concerning national security issues
- the fact that this periodic review is one element of the ISA's processes for democratic oversight of the Agencies.

1.53. We have therefore attempted to write our report in a way that enables it to be read by the public while still containing sufficient detail to provide a realistic setting for our discussion of the issues. To make this report more accessible, we have provided some background details to give lay readers the context necessary to understand the issues discussed.

1.54. At the same time, we have had to deal with the difficulties associated with classified information, which raises particular challenges for engaging in a meaningful way with stakeholders and communities.

[41] BBC "Edward Snowden: Leaks that exposed the US spy programme" (online, 17 January 2014).

CHAPTER 02
Intelligence and security today

Introduction

2.1. This chapter sets the scene for the discussion in subsequent chapters. We briefly address the four matters of:

- the State's need for intelligence
- the impact of rapid technological change
- social license and the intelligence and security agencies
- the human rights framework.

The State's need for intelligence

2.2. Since the publication of the Sir Michael Cullen and Dame Patsy Reddy report (Cullen/Reddy report) in February 2016,[42] there have been numerous reminders of the reasons that Aotearoa New Zealand needs effective intelligence and security arrangements, both nationally and internationally. The terrorist attack on the Christchurch masjidain on 15 March 2019 underscored the country's vulnerability to the threats posed by tech-savvy 'lone actor' extremists. COVID-19 has highlighted the vulnerability of the world's population to pandemics, and the way in which such global events make the public susceptible to incorrect or misleading information (misinformation), information that is deliberately deceptive (disinformation) and conspiracy theories. The increasing use of cyber-attacks by both state actors and criminal groups has highlighted the vulnerability of essential infrastructure and data storage systems within both government and private sector organisations. Russia's invasion of Ukraine, China's increasingly aggressive stance in foreign affairs and the rise of populist politicians with a nativist and authoritarian bent in several important democracies have all underscored the tenuous state of an international order based on the rule of law.

2.3. For a small liberal democracy such as New Zealand, effective intelligence and security arrangements seem vital, not simply to counter threats but also to enable the pursuit of the national interest. Good-quality intelligence helps the government make informed decisions about a wide range of matters – foreign policy, internal and external future threats, defence procurement and so on. In fraught times, informed decision-making becomes particularly important.

---

[42] Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM *Intelligence and Security in a Free Society – Report of the First Independent Review of Intelligence and Security in New Zealand* (February 2016) (*Cullen/Reddy report*).

2.4. As we noted in chapter 1, our country's two intelligence and security agencies (the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS), referred to in our report as 'the Agencies') are expected to contribute to three sets of interests, namely: the protection of New Zealand's national security, New Zealand's international relations and well-being and its economic well-being. Noteworthy for present purposes is the distinction drawn between national security and other interests. We discuss national security in more detail in chapter 5. At this point, we simply note that although New Zealand's current 'all hazards, all risks' approach to national security means a wide range of matters could, in particular circumstances, raise national security concerns, the Agencies' immediate focus will generally be on threats to New Zealand's people and its governmental institutions, structures and processes from malicious actors, either internal or external.[43] This reflects the fact that such protection is a fundamental responsibility of government. For the most part, the Agencies focus their limited resources on foreign interference, counterterrorism and violent extremism, cyber security, global competition and Pacific resilience.

2.5. Governments need intelligence to facilitate good decision-making, especially given today's surfeit of publicly accessible information and rising quantities of disinformation. 'Intelligence' may simply be processed information (often, but not necessarily, secret information), but frequently it will be the result of a complex process that starts with a decision-maker identifying an intelligence requirement and involves collecting and evaluating information (eg, for reliability and accuracy) and then analysing it. An intelligence product may be a one paragraph statement, or something much more complicated, reflecting months of activity by analysts integrating and interpreting a wide range of relevant information and resulting in the production of judgements and forecasts. In relation to intelligence about threats, targeting is usually directed at threat actors. However, the Agencies may draw on a range of other information sources to develop their understanding of threats. This could include using their intrusive powers against individuals who are not themselves threat actors but who can reasonably be expected to provide information about a threat. But the Agencies must obtain the necessary authorisations, which take into account the necessity and proportionality of using their intrusive powers.

2.6. It is important to emphasise in this context that the Agencies should only use their intrusive powers if the government cannot obtain relevant information by less intrusive means. Much relevant information can be obtained through normal government business (for example, from diplomatic posts) or from official sources (such as publications by foreign governments and state entities).

2.7. Moreover, as a result of digitisation and other technological developments, there is more information available from public (or open) sources today than at any previous point in history. In principle, the gathering of such open-source information is lawful, so the Agencies do not need a warrant to collect it.[44] Open-source material includes information published in newspapers, magazines, journals (professional, academic, trade and other specialist journals), over radio or television, on the internet and in government, state entity and company publications of various sorts. Digitisation has not only increased the availability and accessibility of open-source material, but it has also enhanced its utility by, for example, increasing its searchability.

---

[43] As noted in chapter 1, the government has decided in principle to depart from the all hazards, all risk approach to national security in favour of a narrower conception. We discuss this in more detail in chapter 5.

[44] Intelligence and Security Act 2017, s 48.

2.8. An issue we will discuss when we return to the topic of open-source information in chapter 6 is whether there are circumstances in which the Agencies should obtain a warrant to acquire particular information even though it is publicly available (such as information in hacked or leaked data sets).

Impact of rapid technological change

2.9. The world within which intelligence and security agencies operate today is very different from the world they operated in 30 or 40 years ago. The range of possible threats (threatscape) has evolved[45] and will continue to do so as, for example, the effects of climate change are felt on food production, supply chains, population movements and so on. But one area that has had a profound effect on the way we live, on the threatscape we face and on the ability of intelligence and security agencies to counter threats, is rapid technological change.

2.10. Since the 1990s, there have been major developments in communication and associated technologies that have changed the way many New Zealanders live. First, there is the rapid rollout and ongoing development of mobile telephone technology; second, the establishment and development of the internet and the worldwide web and the digitisation of information associated with that; third, the development of an increasing number of internet-connected devices, from tablets and laptops to, more recently, household appliances and vehicles; and fourth, the increasing installation of fibre optic cabling both internationally and nationally.

2.11. These developments have created almost unlimited opportunities for consumers to engage with the internet and the worldwide web, opening up access to a wide range of convenient internet-based tools and services (such as document and photo storage, banking, health care, shopping and multiple sources of news) and access to information on every conceivable subject, like-minded groups (whose members can be engaged in real time wherever they may be based), social media[46] and entertainment, sporting and other platforms.[47] A consequence is that many New Zealanders are increasingly living their lives online, storing their vital information online and making their personal information publicly accessible.

2.12. Overall, there has been an explosion in the amount of accessible information, which has necessitated the development of new tools and techniques for data analysis, such as machine learning and other artificial intelligence technologies. The amount of data created, collected, processed and stored is expected to continue to increase dramatically with the roll-out of 5G-enabled networks.[48]

---

45 For example, the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidian on 15 March 2019 noted that, while the international terrorist attacks perpetrated in the 1990s and early 2000s were primarily carried out by groups in terrorist cells, there had subsequently been an increase in 'lone actor' terrorist attacks, such as occurred in New Zealand in March 2019 (Royal Commission of Inquiry *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) at part 8, chapter 2 [14] (*Royal Commission report*).

46 That is, websites or applications that focus on communication, community-based input, interaction, content-sharing and collaboration, such as Facebook, Twitter, Telegram, Google, Instagram and so on.

47 According to online sources, New Zealand's internet penetration rate stood at 94.9% of the total population at the start of 2022. There were 4.35 million social media users in New Zealand in January 2022 (Simon Kemp "Digital 2022 New Zealand – The essential guide to the latest connected behaviours" (15 February 2022) Datareportal (datareportal.com). The number of mobile phones in New Zealand stands at 5.8 million and exceeds the country's population (L. Granwal "Mobile phone connections in New Zealand FY 2011–2021" (June 30 2022) Statista (statista.com)).

48 Daniel Araya and Meg King *The Impact of Artificial Intelligence on Military Defence and Security* (Centre for International Governance Innovation (CIGI) Papers No 263, March 2022) at 6.

2.13. These developments have not simply facilitated greater consumer convenience and choice; they have also served important societal interests in that they have "boosted freedom of expression, facilitated global debate and fostered democratic participation".[49] But inevitably, there is a price to pay for such benefits. Looking at it from the perspective of individual users, there is the risk of an unintended loss of privacy, with an associated risk of misuse of users' personal data for commercial or other reasons, as well as potential impacts on the exercise of other important human rights. From a societal perspective, the price lies substantially in the internet's capacity to be used by criminals and malicious actors in a variety of ways to further their ends and its adaptability to the creation and widespread dissemination of harmful misinformation, disinformation and extremist views.

2.14. In a 2014 report on privacy, the United Nations High Commissioner for Human Rights noted:[50]

> In the digital era, communications technologies … have enhanced the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection.

Website owners routinely collect data about their users. In some instances, this may improve a user's experience as the website owner will be able to bring information to the user's attention that is relevant to their interests, as revealed by their earlier activities on the website, or to make improvements to the website to reflect user preferences. In other instances, however, users may find that, without their knowledge or informed consent, their personal data is being shared with other website owners or is being sold, either to other website owners or to commercial data aggregators who on-sell it in larger datasets.[51] Similarly, large companies may collect and monetise their customers' data.[52] On-selling of data in larger sets can also be used for criminal/fraudulent purposes; for example, digital doppelgangers.[53]

2.15. Alongside this has been the development and proliferation of increasingly sophisticated means of surveillance – CCTV and similar camera systems, for example, in shops, hotels, universities, schools, sports facilities, public transport, roads and other public and private spaces; video capacity on mobile phones; vehicle and body cameras; smart doorbells and so on. More and more, our images and data are being captured as we go about our daily lives, and we can expect this to increase.

2.16. The scope of these various technological developments has led some commentators to conclude that "surveillance has become the defining characteristic of twenty-first-century society".[54]

---

49 *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights* A_HRC_27_37-EN (30 June 2014) at [1].

50 *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights* A_HRC_27_37-EN (30 June 2014) at [2].

51 For example, Google was able to secretly track the internet activity of Apple iPhone users in late 2011 / early 2012 and collect their data without their knowledge or consent, which it then used for its commercial purposes: see *Google LLC v Lloyd* [2021] UKSC 50, [2021] at [7]–[13].

52 Shoshana Zuboff *The Age of Surveillance Capitalism* (Public Affairs Books, 2019).

53 Criminals buy digital identities on the dark web along with software that allows them to load fake identities onto their computer. Minutes later, they are able to make online purchases, get cash advances and even take over financial accounts undetected, stealing large amounts of money.

54 Lora Anne Viola and Paweł Laidler (eds) *Trust and Transparency in an Age of Surveillance* (Routledge Studies in Surveillance 2021) at 3.

2.17. From the perspective of government agencies involved in intelligence and security, law enforcement and similar work, the technological developments of the last few decades offer a range of significant opportunities and challenges.

2.18. We give examples of opportunities (ignoring questions of lawfulness) below.

- Technology such as big data analytics enables the automated searching of large volumes of data to identify patterns, anomalies or other flags that may be suspicious and require further investigation. Many firms collect and aggregate customer data for a variety of commercial reasons. If they are able to access this data, intelligence and security agencies may be able to obtain valuable information. For example, automated analysis of metadata associated with mobile phone usage (held by telecommunications companies) can provide valuable information about users' daily routines and habits, their interests and preferences, and their relationships, contacts and lifestyles, all without the need to access the content of any calls made or texts sent.
- Biometric technologies, such as automated facial recognition technology, can facilitate effective surveillance and identity-verification activities by intelligence and security and law enforcement agencies, as can optical character recognition technologies.[55]

2.19. Challenges are as follows.

- The system of interconnected networks and devices that makes up the internet offers opportunities for malicious actors to release malware into the system or to attempt to gain access to internet-connected business or government networks or devices to exploit their vulnerabilities. An important part of the work of intelligence and security agencies in many jurisdictions (including New Zealand) is to identify and respond to such malicious activity.
- Technological developments such as automated facial recognition challenge the viability of some traditional tradecraft. As one writer put it: "A cover identity that would have been almost bulletproof only 20 years ago can now be unravelled in a few minutes".[56] (Against that, however, there is an increased ability to create false identities through 'deep fake' technologies.)
- Developments to enhance user privacy (such as encryption and virtual private networks) make the work of intelligence and security agencies more difficult. Over time, quantum computing may affect this, making it easier to break current end-to-end encryption[57] but also perhaps creating opportunities for more effective encryption.

2.20. Rapid technological change also affects the monitoring and oversight of intelligence and security agencies. In particular, to be effective, oversight bodies must have access to sophisticated technical expertise to enable them to understand how the technology works and its potential and possible (less intrusive) technological alternatives. Equally, however, technological developments may provide additional means for oversight bodies to monitor the activities of intelligence and security agencies.[58]

---

55 Optical character recognition (OCR) is the process that converts an image of text into a machine-readable text format. For example, if you scan a form or a receipt, your computer saves the scan as an image file. It can also be used for scanning and reading number plates and road signs in self-driving cars, detecting brand logos in social media posts or identifying product packaging in advertising images.

56 Edward Lucas "The Spycraft Revolution: Changes in technology, politics, and business are all transforming espionage. Intelligence agencies must adapt – or risk irrelevance" *Foreign Policy* (online Spring 2019).

57 See, for example, Jon R Lindsay "Surviving the Quantum Cryptocalypse" (2020) 14(2) *Strategic Studies Quarterly*.

58 See, for example, Kilian Vieth and Thorsten Wetzling "Data-driven Intelligence Oversight – Recommendations for a System Update" (November 2019) *SSRN Electronic Journal 13*.

2.21. The opportunities that modern technologies make available to state agencies raise difficult policy issues. Two real-life international examples involving private-sector companies illustrate some of the interests involved:

- A company creates a substantial database by gathering from the internet personal information that was originally obtained and published by hackers from non-public databases. The company sells access to the database to law enforcement and similar agencies. Among the personal data collected are emails, usernames, passwords, internet addresses and phone numbers, some of which the agencies could otherwise only have obtained under warrant.[59]
- A company scans the internet by automated means to obtain images of people's faces from publicly available websites such as Facebook, YouTube, Venmo and others and applies its facial recognition technology to them. In this way, the company builds up a database holding billions of images and their associated biometric identifiers. It then sells an identification service to law enforcement and other agencies – for example, a law enforcement agency uploads images of people taken at a crime scene; the company applies its facial recognition technology to the images and interrogates its database to see whether there are any matches; the results may help the law enforcement agency identify people involved, whether as offenders, victims or witnesses.[60]

2.22. In the first example, the personal data at issue became publicly available only because hackers obtained unauthorised access to a computer network and improperly copied and published the dataset. From the perspective of the individuals with personal data on the dataset, the critical point is the hacking – the unlawful taking of their private data. That was a clear breach of their interests, defeating what may be a reasonable expectation of privacy in relation to the data. From the company's perspective, however, the critical factor is the availability of the dataset to the public rather than the means by which it became public. This points to an issue to be discussed in chapter 6, namely whether the Agencies should be required to obtain a warrant to acquire publicly available but hacked or otherwise illegally obtained datasets or whether the decisive consideration should be that the dataset is publicly available, with the result that no warrant should be required. Should different principles apply to the hacked confidential information of private citizens than would apply when the hacked information is the confidential information of a close ally?

2.23. In the second example, there is no hacking involved – all the images obtained and processed were publicly available on the websites from which they were gathered. The company had simply gathered images in bulk using an automated search mechanism, applied its facial recognition technology and built a database, to which it sells access. Yet from the users' perspective, there is a substantial difference between posting their images (and/or the images of others) on, say, Facebook to facilitate communication with family, friends and acquaintances (old and new) and becoming part of a commercial database, access to which is sold to a range of users who are prepared to pay for that access. Again, the question is where the decisive interests lie – with the company, which sees itself as simply compiling a database from publicly available information,

---

59 See, for example, Tyler Sonnemaker "Law enforcement agencies are using a legal loophole to buy up personal data exposed by hackers" *Business Insider – Africa* (online 9 July 2020).

60 See, for example, the Privacy Commissioners of Canada, Québec, British Colombia, and Alberta *Joint Investigation of Clearview AI, Inc*. (February 2021), which described indiscriminate 'scraping' of publicly accessible websites as 'unreasonable'.

or with the users,[61] who see their images being monetised and used for a purpose other than the purpose they originally intended; a use they are unlikely to have foreseen.

2.24. Even though the use of this type of technology by intelligence and security, law enforcement and other government agencies will not involve monetisation of people's images, it will involve the use of their images for purposes other than those for which they were initially intended. As the Independent Police Conduct Authority and the Privacy Commissioner pointed out in their recent joint report on the conduct of New Zealand Police (the Police) in photographing members of the public, digital photographs are more than simply images – they are sensitive biometric information.[62] Accordingly, while it may be appropriate for state agencies to utilise such material, such a decision needs to be made after considering the competing interests involved.[63] This includes situations where people's images appear on the internet not because they have posted them there but because others have posted them or they have been the subject of media interest at some stage.

2.25. Similar issues may arise in respect of other technological developments. An example is speaker recognition, which is increasingly being deployed in the business community and is relevant to the work of intelligence and security agencies.[64]

2.26. The developments resulting from rapid technological change of the type outlined above have had two relevant significant effects. First, they contribute to the blurring of the distinction between the work of the security and intelligence agencies and the work of law enforcement agencies.[65] The ability to collect and interrogate vast amounts of information about people from the internet is invaluable to many decision-making agencies within government, so the use of technologies to do this is becoming common across government – the context may vary, but the technological tools utilised are the same.[66] Two recent New Zealand examples illustrate this.

- Immigration New Zealand has been using web crawling technology developed by a private company to monitor Facebook, Instagram, WhatsApp, Twitter and similar platforms to collect users' publicly accessible personal data.[67]
- Police use automated number plate recognition (ANPR) technology from three main sources – their own ANPR cameras, ANPR cameras operated by other government agencies and local bodies, and third-party operators that provide access to number plate information from private-sector companies operating ANPR networks.[68] Police may retain data from ANPR cameras for intelligence purposes for up to 12 months. We were told that the use of ANPR technologies and data is subject to internal approval processes and protocols. In addition,

---

61 Note that not everyone whose image appears on the internet is a 'user' in the sense that they have placed their image on the internet, nor will they necessarily even be aware that their image has appeared online.

62 Privacy Commissioner and Independent Police Conduct Authority *Joint Inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into Police conduct when photographing members of the public* (online 23 September 2022) at 9.

63 As noted above, during our review, the Ministry of Business, Innovation and Employment's (Immigration New Zealand) use of this type of technology received some publicity.

64 Andreas Naustch et al "Preserving Privacy in Speaker and Speech Characterisation" (2019) 58 *Computer Speech & Language* 441.

65 Ales Zavrsnik "Blurring the Line between Law Enforcement and Intelligence, Sharpening the Gaze of Surveillance?" (2013) 9(1) *Journal of Contemporary European Research*.

66 Bernard Marr "The 5 Biggest Tech Trends in Policing and Law Enforcement" *Forbes Magazine* (online, 8 March 2022).

67 Phil Pennington "Immigration NZ enlists 'cyber mercenaries' banned from Facebook to covertly collect data" *Radio New Zealand* (online, 12 October 2022) and Phil Pennington "Government's use of surveillance firm Cobwebs Technologies embroiled in controversy" *Radio New Zealand* (online, 14 October 2022).

68 Phil Pennington "Police step up surveillance activity, tap into CCTV footage from other businesses" *Radio New Zealand* (online, 23 September 2022).

Police have been building up a substantial databank of photographs for future reference and have considered the use of facial recognition technology.[69]

This is not to say that these activities are necessarily wrong or improper. We mention these examples simply to note that they are occurring and that they raise issues similar to those raised in relation to the Agencies. They highlight the risks of looking at the Agencies' activities in isolation from what is occurring elsewhere in government, suggesting that a comprehensive and coordinated analysis will be required at some point.

2.27. The second relevant effect is that technological change has made the distinction between citizens and foreigners much more difficult to maintain. It may no longer be possible to distinguish easily between internal and external threats,[70] and intrusive interception and searching activities, even if aimed at the data of foreigners, are likely to pick up citizens' data as well, given the global interconnectedness of communications systems.

2.28. Determining how to accommodate the competing interests thrown up by the technological capabilities referred to in this section raises the important issue of social licence, to which we now turn.

Social licence and the Agencies

2.29. The Agencies are 'closed shops' in the sense that they deal with classified information in secure environments and the details of the work they do are generally secret. In addition, they have intrusive powers that affect the rights and freedoms of those who live in New Zealand as well as people living elsewhere. The Agencies need the public to accept the legitimacy of their work (and the powers that support it) and to have confidence in the way they go about that work, even though they cannot be fully open and transparent. In short, to be effective, the Agencies need social licence – society's ongoing approval or acceptance of their work.

2.30. Oversight and accountability mechanisms are relevant to social licence. People are more likely to trust the Agencies, or at least accept their legitimacy, if they know that their activities are subject to robust oversight and accountability mechanisms. For example, if people know that the Agencies must obtain the permission of an independent person before they can exercise their intrusive powers or that the Agencies' actions can be scrutinised in an independent and rigorous investigatory process that will result in a public report, they are more likely to accept the legitimacy of the Agencies' work.

---

[69] See Independent Police Conduct Authority and Privacy Commissioner *Joint Inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into Police conduct when photographing members of the public* (September 2022). The Inquiry found that "aspects of both Police policy and practice are inconsistent with [the Privacy Act] framework and breach individual rights. Officers are routinely taking photographs when it is not lawful for them to do so": at [10–11]. See also Nessa Lynch, Liz Campbell, Joe Purshouse and Marcin Betkier *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework* (Law Foundation, November 2020) from [1.5.2].

[70] European Commission for Democracy through Law *Report on the Democratic Oversight of Signals Intelligence Agencies*, 15 December 2015, at [1].

2.31. Before the terrorist attack on the Christchurch mosques on 15 March 2019, the Agencies had limited social licence.[71] As the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019 (the Royal Commission) put it:[72]

> The apparently low threat of terrorism, controversies associated with the intelligence and security agencies and associated public suspicions as to their activities and utility meant that the agencies had limited social licence, political support and funding.

The Royal Commission considered that part of the reason for the Agencies' limited social licence was the lack of informed public debate about national security and the Agencies' work. It saw increased public understanding of, and engagement with, national security issues generally, and with the activities of the Agencies in particular, as key to increasing the Agencies' social licence.

2.32. We acknowledge that the Agencies current Directors-General have been more open with the public about the Agencies' work and the national security, cyber-threat and similar challenges that New Zealand faces than in the past. Both have spoken regularly to public audiences, some outreach work has been undertaken with community groups and, as a general proposition, there is now more information available about the Agencies' activities and the reasons for them. Getting the balance right is difficult, however. The United Kingdom's Intelligence and Security Committee of Parliament has expressed concern about the greater public engagement by agency heads and staff:[73]

> While the Committee recognises the important role public outreach can play in attracting employees by opening up about the culture and working practices in such secret organisations, it must be undertaken in a strategic and considered manner. The Committee is concerned that, if media engagement strategies go too far, they risk trivialising the important work of the Agencies and diverting their focus from national security priorities. Social media is also known to be a battleground for covert hostile state action, so any enhanced media engagement should not undermine the Agencies' ability to act covertly and keep the UK safe.

2.33. As part of our public engagement process, we asked people whether they believed they had enough information about the Agencies and their oversight mechanisms to feel confident that they were working appropriately. The majority did not believe they had enough information or that the Agencies were sufficiently open with the public about their activities. Ethnic and religious community groups we consulted in October and November 2022 described the Agencies as "a black hole" in terms of communicating with communities and akin to "talking to a brick wall". To improve trust in the Agencies and enhance social licence, some respondents suggested strengthening oversight of the Agencies and seeking opportunities for greater public input around national security issues.

2.34. The Agencies' social licence is relevant to our review in at least three ways.

- First, one of the purposes of our review is to consider the recommendations and issues relating to the Intelligence and Security Act 2017 (ISA) raised in the Royal Commission's report. One of Royal Commission's recommendations was that the role of the Intelligence

---

71 As the Agencies note, much of the Government Communications Security Bureau's (GCSB's) work in relation to cyber security is undertaken with consent and would not occur without a degree of social licence on the part of those involved. While that is correct, we are referring here to social licence across the broad range of the Agencies' work. Rather than social licence for a particular aspect of the GCSB's work.

72 Royal Commission report, at part 8, chapter 1 [8a].

73 United Kingdom Intelligence and Security Committee of Parliament *Annual Report 2021-2022* (December 2022) at [28].

and Security Committee should be enhanced; in particular, the Committee should have a more extensive and public role, which would provide "further transparency and general assurance to the public as to the activities of the agencies and thus improve their social licence".[74]

- Second, under our terms of reference, we are required to consider whether the ISA "appropriately balances national, community and individual security with individual privacy and other rights" and "has appropriate protections and oversight in place" for intelligence collection by the Agencies.[75] In this context, issues of 'appropriateness' are ultimately matters of evaluation. Relevant to that evaluation are the views of special interest groups, oversight bodies and members of the public more generally, including views relating to the Agencies' social licence. The terms of reference explicitly recognise the importance of these perspectives by stating that our review will need to meet the communities' expectations of transparency as far as it can and that a wide range of members of the public should have the opportunity to express their views on the issues in our review.
- Third, our terms of reference direct us to take into account "that the review should enhance trust and confidence in the intelligence and security agencies". In other words, enhancing the Agencies' social licence is relevant to how we go about our work.

2.35. We will, therefore, return to the issue of the Agencies' social licence later in this report, particularly when we outline the constraints (including oversight) on the Agencies in chapter 4 and when we make recommendations for improvement in chapter 12.

Human rights framework

2.36. Chapter 1 referred to the democratic paradox, namely that people in liberal democracies accept the need for intelligence and security agencies to protect their political institutions and processes, as well as the democratic values, rights and freedoms they cherish; but they also fear the agencies they set up to do this. As the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police said:[76]

> Liberal democracies face a unique challenge in maintaining the security of the state. Put very simply, that challenge is to secure democracy against both its internal and external enemies, without destroying democracy in the process. Authoritarian and totalitarian states do not have to face this challenge. In such countries there is no need to ensure that security agencies, whose techniques inevitably involve a great deal of secrecy, be accountable to an elected legislature. Nor is there a requirement in such states that all of their security measures be authorized or provided for by law and that none of their officials be above the law. Only liberal democratic states are expected to make sure that the investigation of subversive activity does not interfere with the freedoms of political dissent and association which are essential ingredients of a free society.

2.37. When considering the human rights impact of the activities of intelligence and security agencies, there is a tendency to focus on potential interference with the right to privacy and perhaps also

---

74 Royal Commission report, at part 8, chapter 14 [3.17].

75 The terms of reference are reproduced in appendix A to this report.

76 Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police *Freedom and Security under the Law* (Privy Council Office, Second Report Volume 1, August 1981) at [16].

with freedom of expression. But, as we discuss below, other rights are potentially engaged. That said, we will start with the right to privacy, which:[77]

> … lies at the heart of liberty in a modern state. A proper degree of privacy is essential for the well-being and development of an individual. And restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state …

2.38. Although New Zealand strongly supported the adoption of the United Nations' Universal Declaration of Human Rights[78] and is a party to the International Covenant on Civil and Political Rights,[79] both of which contain a right to privacy, the New Zealand Bill of Rights Act 1990 does not contain an explicit right to privacy. Rather, privacy issues are dealt with through a combination of common law and statute.[80] In particular, privacy interests underlie the protection against unreasonable search and seizure in s 21 of the New Zealand Bill of Rights Act;[81] New Zealand courts have recognised a general tort of invasion of privacy[82] and the Privacy Act 2020 recognises a right to privacy in personal information.[83]

2.39. Given that the Agencies have the ability to exercise intrusive powers against New Zealanders and to capture and store large amounts of personal information, privacy interests are engaged. Although the Agencies are exempt from several of the information privacy principles in s 22 of the Privacy Act, [84] privacy interests are obviously relevant to the way the ISA works. The concepts of necessity, proportionality and absence of less intrusive alternatives that must be considered when intelligence warrants are sought allow for the consideration of privacy interests, as does the power to put conditions on such warrants. Concerns about privacy also underpin other provisions in the ISA, for example, those dealing with the destruction of irrelevant material.

2.40. Apart from examples of the type just mentioned, the ISA recognises explicitly the relevance of privacy interests in various contexts.

- Subpart 2 of Part 5 of the ISA deals with direct access agreements, under which the Agencies can access databases held by other agencies. Before the relevant Ministers can enter into such agreements on behalf of their respective agencies, they must be satisfied that there are adequate safeguards to protect the privacy of individuals,[85] and they must consult with, and invite comment from, the Privacy Commissioner and the Inspector-General of Intelligence and Security.[86]
- Before the relevant Minister can decide to permit an Agency access to 'restricted information', they must conclude that the privacy impact of permitting access is

---

77 *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457 per Lord Nicholls of Birkenhead at [12] (references omitted).
78 Universal Declaration of Human Rights GA Res 217A (10 December 1948), art 12.
79 International Covenant on Civil and Political Rights GA Res 2200A (XXI), art 17.
80 Stephen Penk and Rosemary Tobin (gen eds) *Privacy Law in New Zealand* (Thomson Reuters, Wellington).
81 It underlies other rights as well, eg, the right to freedom of thought, conscience and religion (s 13).
82 *Peters v Attorney-General on behalf of Ministry of Social Development* [2021] NZCA 355.
83 Privacy Act 2020, s 3.
84 Section 28.
85 Intelligence and Security Act 2017, s 126(b).
86 Section 127.

proportionate to the purpose of enabling the requesting agency to perform a ss 10 or 11 function.[87] There are similar provisions in relation to obtaining business records.[88]

- The Inspector-General of Intelligence and Security is entitled to consult with the Privacy Commissioner about any matter relating to the Inspector-General's functions.[89]
- Privacy interests are relevant to the publication of the Agencies' annual reports.[90]

2.41. As we have said, other human rights are also engaged in this context. The ISA recognises this. As noted in chapter 1, under s 17, the Agencies are obliged to act "in accordance with New Zealand law and all human rights obligations recognised by New Zealand law". One particular set of rights, freedom of expression (which is protected by s 14 of the New Zealand Bill of Rights Act) is singled out for particular mention in the ISA. Section 19 provides:

> **Activities of intelligence and security agency not to limit freedom of expression**
>
> The exercise by any person in New Zealand or any class of persons in New Zealand of their right of freedom of expression under the law (including the right to advocate, protest, or dissent) does not of itself justify an intelligence and security agency taking any action in respect of that person or class of persons.

2.42. The Royal Commission considered that s 19 could be interpreted in a way that hindered the Agencies' ability to undertake legitimate target discovery activities and recommended that the section be given further consideration. We address that issue in chapter 5.

2.43. In terms of the relevance of human rights other than privacy, commentators and submitters to this review, have pointed to the chilling effect that large-scale surveillance activities by intelligence and security agencies can have on the populace and the risk that presents to the functioning of democracy.[91] They argue that people refrain from engaging in some types of lawful conduct out of fear that it might attract the attention of intelligence and security agencies:[92]

> The rights to freedom of opinion, freedom of expression, freedom of association, freedom of assembly, and freedom of thought, conscience, and religion are all directly affected. Importantly, the effects in this area may be cumulative and not just felt at an individual level. It is the effect on privacy, opinion, expression, association, assembly, thought, conscience, and religion as inter-dependent rights with society-wide implications that is at issue. The harm cannot be considered fully by analysing these rights in isolation, as it is the combination of the rights that serve to protect and facilitate the functioning of democracy.

We agree that it is important to consider the effect on rights in this interconnected way.

2.44. As part of our public engagement process, we asked whether people believed the ISA has the right balance between security interests and the rights and freedoms of New Zealanders. Most respondents did not believe the balance is right and felt the system is tilted too far towards the

---

87 'Restricted information' is information that has additional protections under other legislation. It is defined in s 135 of the ISA and includes information specified in the Tax Administration Act 1994; the Education and Training Act 2020; the Births, Deaths, Marriages, and Relationships Registration Act 1995 and the Land Transport Act 1998.

88 Intelligence and Security Act 2017, s 147(2)(b).

89 Section 161(2).

90 Section 221(5)(e).

91 See, for example, Daragh Murray, Pete Fussey, Lorna McGregor and Maurice Sunkin KC "Effective Oversight of Large-scale Surveillance Activities: A Human Rights Perspective" (2021) 11 J of *Nat Sec Law & Policy 743* at [760–761].

92 Above n, at [761].

Agencies. When asked to rank a closed list of activities that could help improve the balance, the highest number of respondents indicated 'increasing oversight' as being most helpful, followed in order by 'having more limits on what Agencies can look into', 'more public input into overseeing the agencies' and 'having more visible public reporting'.

2.45. Chapter 7, which addresses the warranting framework under which the Agencies are entitled to use their intrusive powers, provides more information on the views from our public engagement process around impacts on rights and freedoms.

SECTION 02

New Zealand's intelligence and security system

CHAPTER 03

Aotearoa New Zealand's national security and intelligence community: An overview

Introduction

3.1. In this chapter, we give an overview of Aotearoa New Zealand's national security and intelligence community. Without a definitive definition of the community and with some disagreement as to where particular agencies sit within it, this is not a straightforward exercise.

3.2. We begin with what we will describe as the 'core' intelligence and security agencies. These are the agencies recognised in the Intelligence and Security Act 2017 (ISA), ie, the Department of the Prime Minister and Cabinet (DPMC) (in particular, the National Assessments Bureau or NAB), the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS).[93] We then go on to describe other important agencies, such as the intelligence function within the New Zealand Defence Force (NZDF) and that within the New Zealand Police (Police), before outlining the broader intelligence community. We then highlight some issues relating to coordination and coherence within the broader intelligence community.

3.3. We give this overview for three reasons.

- First, to understand the roles of the core agencies, we must place them in the context of the wider intelligence and national security community. This helps in evaluating the ISA and in considering some of the issues raised in our terms of reference.
- Second, our discussions with various agencies that form part of the wider intelligence and security community have revealed gaps in their legislative frameworks, which have led to understandable but undesirable work-arounds. These need to be resolved. In addition, there are inconsistencies in relevant legislative frameworks.
- Third, our inquiries have also revealed potential difficulties with the way the cooperation, advice and assistance provisions in the ISA are being interpreted and applied. The earlier review carried out by Sir Michael Cullen and Dame Patsy Reddy (the Cullen/Reddy review)[94] concluded that there should be greater cooperation and engagement between the GCSB and the NZSIS on one hand and the 'broader public sector' on the other, noting:[95]

---

93 Throughout our report, we refer to the NZSIS and the GCSB as 'the Agencies'.

94 Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM *Intelligence and Security in a Free Society – Report of the First Independent Review of Intelligence and Security in New Zealand* (February 2016) (*Cullen/Reddy report*).

95 Above n, concluding remarks at [147].

> Intelligence is only useful to the extent that it can be used by other public authorities and ministers to inform decisions and actions. At times the Agencies will need to work closely with agencies such as Police and the Defence Force to enable this …

3.4. We address this point in chapter 10.

Preliminary matters

3.5. Before we begin the overview, we mention two preliminary matters.

- First, in October 2014,[96] the government separated ministerial responsibility for national security and intelligence as a whole from ministerial responsibility for the GCSB and the NZSIS. As a consequence, as at 2022, the Prime Minister is the Minister for National Security and Intelligence and has responsibility for the overall direction, policy and oversight of the broad national security and intelligence sector. Meanwhile, Hon Andrew Little is the Minister Responsible for the GCSB and the NZSIS and, in that capacity, has various responsibilities under the ISA, including considering applications for warrants.
- Second, New Zealand is a member of the Five Eyes intelligence partnership.[97] New Zealand's membership of the partnership is relevant to some of the matters dealt with in the ISA, such as intelligence priority setting and the handling of classified information.

3.6. In brief, the Five Eyes is an intelligence partnership between Australia, Canada, New Zealand, the United Kingdom and the United States of America (the United States). This partnership grew out of a treaty between the United States and the United Kingdom to coordinate and share 'signals intelligence' (SIGINT).[98] New Zealand's membership of Five Eyes is highly valued by the New Zealand government, although it has at times been controversial. As noted in the Cullen/Reddy report:[99]

> Intelligence partnerships … help New Zealand prioritise and focus intelligence collection and assessment resources on the areas most important to us, while avoiding intelligence gaps.

3.7. As would be expected given the relative size and importance of its members, New Zealand obtains far more information from the partnership than it provides. The Cullen/Reddy report notes:[100]

> For every intelligence report the NZSIS provides to a foreign partner, it receives 170 international reports. Similarly, for every report the GCSB makes available to its partners, it receives access to 99 in return … Of all security leads the NZSIS investigates, around half are received from foreign partners. These represent possible threats to the security of New Zealand, most of which we would not be able to discover on our own (for instance, because they have a foreign source).

---

96 Department of the Prime Minister and Cabinet "National Security and Intelligence Role Created" (press release, 6 October 2014).

97 The material in relation to Five Eyes is drawn principally from the Cullen/Reddy report at [3.42]–[3.47] and [4.27]–[4.28].

98 British-United States communication intelligence agreement signing on 5 March 1946, originally known as the BRUSA Agreement but now known as the UKUSA Agreement.

99 Cullen/Reddy report, at 45.

100 Cullen/Reddy report, at 45. A similar ratio applies to New Zealand's defence intelligence and central intelligence assessment functions.

3.8. Membership of Five Eyes is important to the work of the GCSB in particular and the NZSIS (referred to in our report as 'the Agencies'), as well as to the intelligence and national security community more generally. However, the relationship is not one way: we understand that foreign partners seek New Zealand's assistance with intelligence gathering and that New Zealand is able to make significant contributions in some areas.

3.9. Collaboration between the Five Eyes countries has moved beyond just intelligence over the course of the partnership and now includes border security, defence and police activities. Ministers with responsibility for domestic security meet regularly as the 'Five Country Ministerial'. In addition to regular Five Eyes ministerial meetings and intelligence and assessment exchanges, there are meetings between specialist groups from the five countries (national security agencies, border agencies, oversight bodies, technical experts and so on) alongside the sharing of skills, technology and capability.[101]

3.10. As the Cullen/Reddy report noted,[102] along with the benefits, there are risks and costs associated with membership of Five Eyes. There is, for example, the risk of losing some independence in relation to intelligence, defence and foreign policy settings. It is improbable that New Zealand's national interests will coincide exactly with those of other countries, even friendly ones.[103] In addition:

- membership of Five Eyes may increase the risk of New Zealand becoming the target of foreign interference[104]
- each international agency's information is treated as their information and will not be made more widely available without their consent. Similarly, the New Zealand Agencies set conditions for sharing their information with foreign partners in order to protect it. This approach can cause difficulties with accessing relevant information in a timely way.[105]

New Zealand's core national security and intelligence agencies

3.11. New Zealand's core national security and intelligence community of the GCSB, the NZSIS and the NAB within DPMC are the agencies that produce intelligence and assessment for the whole of government and perform a range of functions established by the ISA. The principal objectives of the Agencies are to contribute to three sets of interests: the protection of New Zealand's national security, New Zealand's international relations and well-being and its economic well-being.[106]

---

[101] For example, border cooperation: Gill Bonnett "Plans for touchless border for Five Eyes citizens" *Radio New Zealand on 1 News* (online,23 October 2022).

[102] Cullen/Reddy report, at [4.28].

[103] A similar concern emerged in some of the submissions and comment we received, to the effect that New Zealand's membership of Five Eyes, the amount of material received and the values underpinning its collection may impact the Agencies' focus and assessment of threats to New Zealand.

[104] Miriam Wharton "The Development of Security Intelligence in New Zealand, 1945–1957" (Master of Defence Studies Thesis, Massey University, 2012) at 28: "Being less able to protect the increasing flow of secrets they handled, states like New Zealand became targets for Soviet espionage despite their own relative insignificance"; Dan Satherley "NZ labelled soft underbelly of Five Eyes Spy Network in Canadian report" *New Zealand Herald* (online 31 May 2018); Global Times Editorial "Five Eyes 'dim-sighted' when hyping China infiltration" *China Global Times* (online 19 June 2022): "A decades-old Chinese song goes like this, 'Fine wine for friends and shotguns for jackals.' Be it Five Eyes or Ten Eyes, as long as they dare damage China's interests, they will definitely get themselves into trouble.".

[105] See, for example, Inquiry into Operation Burnham, 17 July 2020 (minute no. 25).

[106] Intelligence and Security Act 2017, s 9.

3.12. We will briefly outline the roles of DPMC and the Agencies. Following that, we will describe elements of the broader intelligence and national security community.

Department of the Prime Minister and Cabinet

3.13. In relation to national security and intelligence, DPMC supports the Prime Minister in their role as Minister for National Security and Intelligence. DPMC also supports the Minister Responsible for the GCSB and NZSIS in certain matters. Some of the specific functions DPMC performs are referred to in the ISA, but many are not. These aspects of DPMC's work are carried out through a business unit, the National Security Group.

3.14. Under s 233(1) of the ISA, the chief executive of DPMC is responsible for the performance of three functions, that is:

- providing intelligence assessments on events and developments of significance to New Zealand's national security, its international relations and well-being and its economic well-being to Ministers, departments, interdepartmental ventures and others considered appropriate by the chief executive
- advising Ministers on the setting of priorities for intelligence collection and analysis
- advising departments on best practice in relation to the assessment of intelligence.

3.15. However, under s 233(2), the chief executive is prohibited from carrying out the first and third of these functions personally but rather must designate an employee to carry them out. Section 234 directs that employee to act independently in matters relating to these two functions. The designated employee heads the NAB, which undertakes intelligence assessments and is a unit of the National Security Group.

3.16. The National Security Group is headed by a deputy chief executive who is responsible to the chief executive for matters of national security policy. The designated employee who heads the NAB reports to the deputy chief executive.

3.17. DPMC also administers the ISA, supports Parliament's Intelligence and Security Committee and is responsible for coordinating and implementing recommendations from the Royal Commission of Inquiry into the terrorist attacks on Christchurch masjidain on 15 March 2019 (the Royal Commission).

3.18. The advice that DPMC provides in relation to setting intelligence priorities culminates in the National Security Intelligence Priorities (NSIPs), which are approved by Cabinet.[107] DPMC coordinates the National Intelligence Coordination Committee to develop and oversee the NSIPs. DPMC acts as both the chair and secretariat of the committee. The NSIPs guide and facilitate coordination of effort across the 10 agencies that sit on the committee, ie, Ministry of Business, Innovation and Employment (MBIE), the New Zealand Customs Service (Customs), the NZDF, Police, New Zealand Ministry of Defence, Ministry of Foreign Affairs and Trade (MFAT), Ministry for Primary Industries (MPI), NAB, GCSB and NZSIS. The NSIPs are stated at a high level of generality, allowing the Agencies discretion to provide intelligence on issues "that align with their individual capabilities, resources, and mandates".[108]

---

[107] There is a classified version and a publicly available version. For the latest publicly available version, see the New Zealand Government's National Security Intelligence Priorities 2021 (November 2021).

[108] Department of the Prime Minister and Cabinet "National Security Intelligence Priorities" (online, 16 December 2021).

3.19. DPMC is also the lead national security and intelligence policy adviser to the government, which we discuss further in chapter 5.

National Assessments Bureau

3.20. The NAB is New Zealand's primary intelligence assessment agency, albeit not the country's only intelligence assessment body. It fulfils the two functions that the chief executive of DPMC is prohibited from performing personally, namely:[109]

- providing intelligence assessments on New Zealand's national security, international relations and well-being and economic well-being to the Prime Minister and Cabinet, government departments and any other person who the chief executive of the DPMC considers appropriate
- advising departments on best practice in relation to assessing intelligence.

3.21. The NAB provides all-source intelligence assessment, which means that it assesses all available information from public, official and intelligence sources. One stream of information is secret intelligence and assessment, including SIGINT, human intelligence (HUMINT) and geospatial intelligence (GEOINT). However, most information assessed is not secret; it is restricted official information and assessment reporting from domestic and international agencies and public sources, such as public websites and official publications, as well as all forms of media, scientific, expert and academic commentary and publications. The NAB is purely an assessment agency – it does not collect intelligence, nor does it make recommendations for action.

3.22. The requirement in s 234 for independence is intended to ensure that the NAB's intelligence assessments provide an impartial perspective on developments and risks to New Zealand at a strategic level. The NAB aims to adhere to rigorous analytic standards that mitigate bias and to undertake deep research and analysis of contemporary and historical information. Independence and impartiality in the intelligence assessment function is vital.[110] If intelligence assessments are 'shaded' for political purposes, the public will sooner or later lose confidence in the reliability and integrity of the intelligence assessment process, which will likely undermine public acceptance of decisions made on the basis of such assessments.

3.23. As the government's primary agency for intelligence assessment, the NAB is also responsible for advising departments on best practice in relation to intelligence assessment, although we understand this function is yet to be implemented in practice.

3.24. In 2021, the NAB reconstituted a National Assessments Committee, the history of which is discussed in some detail in the Royal Commission report.[111] Convened by the director of the NAB, this monthly meeting is a voluntary forum for exchanging views on national assessments matters, including the work programmes of participating agencies, in addition to the National Intelligence Coordination Committee mentioned earlier.[112]

---

[109] Intelligence and Security Act 2017, s 233(1).

[110] Sir John Chilcot and a Committee of Privy Counsellors *The Report of the Iraq Inquiry: Executive Summary* (United Kingdom House of Commons, 6 July 2016) at [808] and [842]–[848].

[111] Royal Commission of Inquiry *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) at part 8, chapter 4 [15] (*Royal Commission report*).

[112] Other groups undertaking intelligence assessments include the multi-agency Combined Threat Assessment Group hosted within the NZSIS, New Zealand Defence Intelligence (NZDI) within the NZDF, as well as the relevant business units within MBIE, MPI, Customs and Police.

3.25. Finally, the NAB can, where authorised by its director, provide New Zealand's foreign partners with intelligence assessments it has produced and act as a conduit for disseminating intelligence assessments from its international partner agencies to the New Zealand government, in line with partner controls.

The Agencies

3.26. Before we address the GCSB and the NZSIS individually, we note one of their important shared functions is to collect and analyse intelligence in accordance with the government's priorities. The GCSB and the NZSIS provide intelligence to help government entities perform their functions: with the entities including the NAB, the NZDF, the Ministry of Defence, Customs, Police, MFAT, MPI, MBIE and the Serious Fraud Office. The information can help with decision-making about threats and risks to national security and about the advancement of New Zealand's interests.

3.27. In addition, the GCSB and the NZSIS, where authorised, provide intelligence they have collected to New Zealand's foreign partners and act as a conduit for disseminating intelligence from their international partner agencies to the New Zealand government, in line with partner controls.

3.28. The GCSB and the NZSIS operate within a statutory framework that, among other things, identifies fundamental principles with which the Agencies are expected to comply as they undertake their activities. We describe these principles in chapter 4.

Government Communications Security Bureau

3.29. The GCSB is New Zealand's primary SIGINT Agency, which means that it specialises in providing intelligence derived from electronic communications. The GCSB identifies, collects, analyses and reports on data, including communications such as phone calls, emails and social media posts. The GCSB also shares intelligence obtained from international partners to the whole of government and has a cyber-security function, as discussed below.

National Cyber Security Centre

3.30. The main way that the GCSB provides cyber-security services is through its National Cyber Security Centre. The centre helps government agencies and private sector organisations of national significance protect and defend their information systems against cyber-borne threats that are typically beyond the capability of commercially available products and services. It supplies advanced cyber-threat detection and disruption and cyber-protection capabilities to these organisations. This includes responding to high-impact cyber incidents at the national level; managing the government's information security standards and producing cyber-threat intelligence assessment reporting.

3.31. Within the centre, there are also technical experts who contribute advice and expertise towards national security and intelligence functions under other legislation, including provision of risk assessment under the Telecommunications (Interception Capability and Security) Act 2013, the Outer Space and High-altitude Activities Act 2017, the Overseas Investment Act 2005 and the Radiocommunications Act 1989. The GCSB is prohibited from enforcing measures for national security except in relation to its information assurance and cybersecurity activities.[113] In respect of those activities, the GCSB is entitled to do:[114]

[113] Intelligence and Security Act 2017, s 16(a). In addition, the GCSB may take enforcement measures in the context of performing its functions under s 13 or where another Act permits it.

[114] Section 12(1)(b).

> ... everything that is necessary or desirable to protect the security and integrity of communications and information infrastructures of importance to the Government of New Zealand, including identifying and responding to threats or potential threats to those communications and information structures.

3.32. The GCSB is the authority for the government's classified information systems, helping protect classified government information from unauthorised disclosure and keep government communications secure. The Director-General of the GCSB also now acts as the Government Chief Information Security Officer, which means that the GCSB provides information security policy advice, sets the government's information security standards and provides services to other government agencies and departments.

New Zealand Security Intelligence Service

3.33. The NZSIS is New Zealand's primary HUMINT agency, specialising in providing intelligence derived from people. The NZSIS investigates, collects, analyses and reports on intelligence obtained from people directly and through a range of other collection methods, including open-source discovery and research, human intelligence, physical surveillance and technological surveillance such as tracking and listening devices. The NZSIS also shares HUMINT obtained from international partners with the whole of government.

3.34. NZSIS has a strong focus on security intelligence, namely intelligence on the identity, capability and intentions of hostile individuals or organisations that may be engaged in activities such as espionage, foreign interference, sabotage or terrorism and violent extremism. This may include working with Customs regarding people crossing the border and with Immigration New Zealand regarding visa and residency screening, including providing risk assessments to Immigration New Zealand.

3.35. Another important function of the NZSIS is to provide protective security services, advice and assistance to the government to help protect people, information and assets. The main tool for this is the Protective Services Requirements (PSR) framework, which is a policy framework mandated by Cabinet that sets out what government agencies must do to manage their security effectively. It covers security governance and personnel, physical and information security. These requirements are publicly available.[115] The NZSIS also provides the government's security vetting (or clearance) function, assessing an applicant's suitability to hold a national security clearance and providing recommendations to government agencies about protecting access to information, assets and work locations that could affect New Zealand's security interests.

3.36. The Combined Threat Assessment Group (CTAG) hosted by the NZSIS is an interagency group that provides threat-based intelligence assessments.[116] These assessments address the terrorism threat to New Zealand, including violent extremism in advance of any terrorist acts, as well as threats from violent protest and violent crime abroad. CTAG's intelligence assessment insights about terrorism threats contribute to Police and NZSIS operations and to the NAB's strategic assessment of the risk of terrorism. CTAG threat reporting is also used by other government agencies that set security standards for their sector (such as the Civil Aviation Authority or Immigration New Zealand).

---

[115] Protective Security Requirements "Mandatory requirements" (online, May 2022), (protectivesecurity.govt.nz/governance/mandatory-requirements/).

[116] The group has included seconded staff from the NZSIS, NAB, Police, NZDF and MFAT.

3.37. The NZSIS sets New Zealand's national terrorism threat level that, amongst other purposes, can influence government decision-making.[117]

Other national security and intelligence agencies

3.38. Two major partners of the GCSB, NZSIS and NAB are referred to specifically in the ISA – the NZDF and the Police.

3.39. Other agencies with important national security and intelligence capabilities not referred to in the ISA include MFAT, the Ministry of Defence, Customs and MBIE (which includes Immigration New Zealand). These agencies are all members of the government's principal strategic national security decision-making group, the Security and Intelligence Board.[118] They advise on intelligence priorities and requirements, make recommendations and take action based on intelligence and assessment, including in some cases, enforcement measures. These agencies can provide significant information and are the largest users of the products and services of the GCSB, the NZSIS and the NAB. Except for MFAT and the Ministry of Defence, all have dedicated and growing intelligence and assessment capabilities for their internal purposes.

3.40. There are other New Zealand agencies that are part of a wider intelligence community. Some have established or expanded their own dedicated intelligence and assessment capabilities to support policy making and law enforcement. In 2021, officials undertook an intensive stocktake of how some intelligence agencies contribute resources against each NSIP, which has started to build a picture of their efforts.[119] This wider intelligence community, which may not have national security as a principal function, includes MPI, the Department of Corrections, the Environmental Protection Authority, the Department of Internal Affairs, the Civil Aviation Authority of New Zealand, Maritime New Zealand and agencies that focus on social well-being, such as the Ministry of Social Development and, most recently, the Ministry of Health.

3.41. The NZDF and Police, as the only other agencies referred to in the ISA, are significant for two reasons.

- First, the GCSB and NZSIS must cooperate with the Police and NZDF as they are major operational agencies that implement enforcement measures, which the GCSB and NZSIS generally cannot. Under s 16 of the ISA:

> It is not the function of an intelligence and security agency to enforce measures for national security except as may be required—
>
> (a) in connection with any information assurance and cybersecurity activities that are carried out by the Government Communications Security Bureau; or
>
> (b) in the course of performing its functions under section 13; or
>
> (c) under any other enactment.

---

[117] In November 2022, the NZSIS announced that New Zealand's terrorism threat level had been dropped from medium to low, meaning a terror attack is now deemed "a realistic possibility" instead of "feasible and could well occur". See, Thomas Manch "New Zealand's terror threat level drops from 'medium' to 'low'" *Stuff* (online, 30 November 2022).

[118] The Security and Intelligence Board is made up of the chief executives of MFAT, Customs, MBIE, Police, the Ministry of Defence, the NZDF and DPMC as well as the GCSB and NZSIS. The NAB is not a member, however the director of the NAB reports to the deputy chief executive of DPMC (National Security Group), who is a member. The Treasury was previously a member of the forerunner of this committee but no longer participates.

[119] Cabinet Paper "2021 updated National Security Intelligence Priorities – Whakaarotau Marumaru Aotearoa – for approval and overview of improvements to date" (December 2021).

- Second, the NZDF and the Police have their own significant national security and intelligence collection and assessment capabilities.

Defence

3.42. Here, we discuss the NZDF, including New Zealand Defence Intelligence (NZDI), and the Ministry of Defence. Before we do so, however, we note that powers in relation to the defence of New Zealand come from various sources: from statute, from the Royal (or Crown) Prerogative[120] and from international law. In some instances, it is not clear precisely where a particular power is located.

New Zealand Defence Force

3.43. Under the Defence Act 1990, the NZDF has a broad mandate to defend and protect the interests of New Zealand, both in New Zealand and elsewhere. In addition, the NZDF can provide "assistance to the civil power either in New Zealand or elsewhere in time of emergency" and "any public service".[121] The Chief of Defence Force is the principal military adviser to the Minister of Defence and other Ministers and is responsible for carrying out the functions and duties of the NZDF (including those imposed by any policies of the government), including by issuing Defence Force Orders under s 27 (1) of the Defence Act.

3.44. This means that the NZDF performs a critical national security and intelligence function at home and abroad. It undertakes military operations and training at sea, on land and in the air both nationally and around the world. New Zealand has one of the largest exclusive economic zones to defend and protect, responsibilities for the Cook Islands, Niue and Tokelau and interests in Antarctica. The NZDF's COVID-19 operation was the largest commitment of NZDF personnel to support the civil power in more than 50 years, with over 6,200 personnel involved in providing operational planning, security and management of managed isolation and quarantine facilities across the country.

New Zealand Defence Intelligence

3.45. NZDI works closely with the NAB, the GCSB and the NZSIS, but it is not governed by the ISA; it is not defined as a national security and intelligence agency, nor is it explicitly mentioned in the Defence Act or any other statute. The Defence Act does not define or set out the functions and powers of defence intelligence staff.

3.46. However, reflecting the broad purposes of the NZDF under the Defence Act, a Defence Force Order has been issued setting out "the policies and direction to be followed when conducting NZDF Intelligence activities".[122] The purpose of the Order is to:

a. ensure that all Defence Force Intelligence activities are conducted lawfully;

b. authorise the conduct of Defence Force Intelligence activities;

c. set out the policies and responsibilities for Defence Force Intelligence;

---

[120] The Royal Prerogative (sometimes called the Crown Prerogative) refers to the Sovereign's customary authority and power as recognised by the common law. To the extent that it still exists, the Royal Prerogative is in fact exercised by the government of the day.

[121] Defence Act 1990, s 5(e) and (f).

[122] Chief of Defence Force "Defence Order 21: Defence Intelligence" (21 March 2022) Authority Order.

d. provide a set of principles designed to ensure strategic alignment and a consistent approach to Defence Force Intelligence throughout the NZDF; and

e. empower the making of subordinate policies to manage Defence Force Intelligence, including acceptable use policies.

3.47. The legal basis for defence intelligence operations is stated to be "the Defence Act, other New Zealand legislation, international laws and elements of common law, including the Crown Prerogative".[123]

3.48. There is some statutory recognition of the fact that the NZDF undertakes surveillance and intelligence-gathering activities. Section 133A(1) of the Radiocommunications Act 1989 creates offences in relation to the disclosure of certain radiocommunications124 or information from them. Section 133A(2)(d) clarifies that this does not apply to "any radiocommunications intercepted by a member of the New Zealand Defence Force, in connection with any of the purposes specified in sections 5(a) to (d) of the Defence Act 1990". Section 133A(4) makes it plain, however, that s 133(2) "does not authorise the interception of any private communications within the meaning of section 216A of the Crimes Act 1961".

3.49. Under the Defence Act, the Chief of Defence Force may delegate any functions, duties and powers. In practice, the function of strategic and specialised intelligence is delegated to the Chief of Defence Intelligence, who commands NZDI and reports to the Vice-Chief of the Defence Force. Other elements of the NZDF also have operational and tactical intelligence capabilities. NZDI provides the strategic and specialised component of the wider NZDF intelligence enterprise.

3.50. In addition, where authorised, NZDI provides intelligence and intelligence assessments to New Zealand's foreign partners and acts as a conduit for disseminating intelligence from international partner agencies to New Zealand's government, consistently with partner controls.

3.51. NZDI has four functions directly related to national security and intelligence.

- NZDI provides strategic intelligence leadership for the NZDF intelligence enterprise, which includes NZDI and the other intelligence elements in the NZDF. NZDI uses the NSIPs as a basis for setting its own intelligence priorities, concentrating on the NSIPs most relevant to defence or critical to functioning, like force protection. NZDI uses this plan to influence intelligence and assessment production across NZDF.
- NZDI is the primary provider of strategic military intelligence assessment to the Minister of Defence and other Ministers; to the Chief of Defence Force and the chiefs of the three services (army, navy and air force) and to other government agencies, principally the Ministry of Defence and MFAT. NZDI focuses on developments and events of military interest, including foreign military capabilities and intentions. For example, NZDI provides a military intelligence assessment to inform Ministerial decision-making on deployments.
- NZDI is the national authority for GEOINT.[125] While the NZDF remains the main user of classified GEOINT, in recent years, changes in technology have enabled other government

[123] Chief of Defence Force "Defence Order 21: Defence Intelligence" (21 March 2022) Authority Order.

[124] 'Radiocommunications' is defined under the Radiocommunications Act 1989, s 2, to mean "any transmission or reception of signs, signals, writing, images, sounds, or intelligence of any nature by radio waves".

[125] GEOINT is based on a specialised collection of data from satellites and airborne and hand-held devices. GEOINT products analyse geospatial information and imagery and describe, assess and visually depict physical features and geographically referenced activities on land and sea and in the air and space. For example, for humanitarian assistance and disaster relief in the Pacific, GEOINT New Zealand Data Service provides pre-event baseline imagery and analyses to identify damage.

agencies to establish their own GEOINT capabilities, for example, Toitū Te Whenua (Land Information New Zealand or LINZ).

- NZDI provides specialised intelligence support to military operations in armed conflict and in peacetime. The NZDF's authorisation framework for intelligence activities is not set out in legislation but is contained in Defence Force Orders and instructions and can include approval at the ministerial and Prime Ministerial levels. In addition, where requested by the Agencies, NZDF may help the Agencies give effect to an authorisation pursuant to section 51 of the ISA.

Ministry of Defence

3.52. Under the Defence Act 1990, the Secretary of Defence is the principal civilian adviser to the Minister of Defence and other Ministers and has a range of national security functions, including to formulate advice on defence policy and to manage procurement, replacement and repairs of military capabilities. Of most relevance to the ISA is the secretary's function under the Defence Act 1990 to "prepare, in consultation with the Chief of Defence Force, and submit to the Minister from time to time a defence assessment, including a review of different options capable of achieving the government's policy goals".[126]

3.53. In practice, major defence assessments have typically been produced about once every five years and are one of the few strategic analytic products about New Zealand's position in the world that the government shares with the public. According to the Ministry of Defence website, this assessment function has expanded in scope and size to "consider major strategic trends, as well as more in-depth, emerging and evolving issues that could affect New Zealand's national security interests" to ensure that the Ministry and the NZDF are "better able to keep pace with and respond to changes in New Zealand's security environment".[127]

Police

3.54. Under the Policing Act 2008, Police have a range of functions, including in relation to national security.[128] Their work may sometimes overlap with the work of the Agencies. The Policing Act acknowledges the important and valuable role others can play in how the Police perform their functions, and that it is often appropriate that, when performing their functions, the Police cooperate with other agencies.[129] The Policing Act also includes principles: that require Police services to be provided "in a manner that respects human rights" and are "independent and impartial", requires every employee to act professionally, ethically and with integrity and directs the Police to obtain a "wide measure of public support and confidence" to be effective.[130]

3.55. The Police Commissioner is responsible to the Minister of Police for the functions and duties of the Police and the general conduct and management of the Police but must act independently of the Minister in relation to the maintenance of order, enforcement of the law, investigation and prosecution of offences and decisions about individual employees. Under the Policing Act, the commissioner may delegate functions. In practice, operational command of the Police is delegated to 12 district commanders.

---

[126] Defence Act 1990, s 24(c).
[127] Ministry of Defence "Defence Assessments" (defence.govt.nz).
[128] Policing Act 2008, s 9(f).
[129] Section 10.
[130] Policing Act 2008, s 8 (b).

National Intelligence Centre

3.56. The intelligence and assessment capability of the Police is not provided for in the Policing Act, but the Police base it on their function of crime prevention under s 9. They define the purpose and role of intelligence as provision of "timely, accurate, and relevant insight and foresight to enhance tactical, operational and strategic decision-making".[131]

3.57. The production of intelligence and assessment within Police is shaped by the requirements of applicable legislation, including the Search and Surveillance Act 2012, the Evidence Act 2006, the New Zealand Bill of Rights Act 1990, the Privacy Act 2020 and the Criminal Procedure Act 2011. Intelligence must be actionable and capable of being presented in a way that makes it useable in a court setting. This means that intelligence and assessment is generally produced by Police at a classification level no higher than restricted, although some Police can access all levels of classified information.

3.58. The Police Commissioner's strategic intelligence function is delegated to the Director National Intelligence, who reports to an assistant commissioner and leads the National Intelligence Centre, a group of around 100 intelligence personnel. District commanders lead operational and tactical intelligence personnel. Specialised intelligence and assessment units are embedded in relevant strategic groups, such as the National Security Investigation Team, Financial Intelligence Unit, Human Source Management Unit and the Transnational Crime Unit. The Gang Harm Insights Centre is a multi-agency unit supporting the government's strategic response to the harm caused by organised crime. Participating agencies have an approved information sharing agreement under the Privacy Act 2020.

3.59. The National Intelligence Centre has two main functions directly related to national security and intelligence.

- It provides the strategic coordination and direction of the wider Police intelligence capability. It uses the NSIPs to help set Police intelligence priorities and develop Police intelligence capabilities, with a focus on priorities that are most relevant to Police, such as terrorism and violent extremism and transnational crime. The centre oversees intelligence collection and promotes the production of relevant intelligence and assessment, including by disseminating intelligence requirements to Police in the field. It also provides Police training in intelligence, alongside the Royal New Zealand Police College.
- The centre is also the primary provider of strategic intelligence and assessment to the Police Commissioner and other senior Police personnel. It focuses on priorities of Police interest. It has specific intelligence capabilities that focus on national security and intelligence threats and recently established an open-source intelligence team.

New Zealand Customs Service

3.60. Under the Customs and Excise Act 2018, the principal purpose of Customs is to levy and collect excise duty and administer, enforce and facilitate customs controls at the New Zealand border in relation to the arrival of goods, people and craft, including prohibiting the importation of offensive material and exports of nuclear, biological and chemical weapons. Customs also has a role under numerous other laws, many of which relate to national security, such as the Terrorism Suppression Act 2002 and Immigration Act 2009.

---

[131] New Zealand Police *Enabling the New Zealand Police Deployment Model: National Intelligence Operating Model 2021* (2021) at 7.

3.61. Customs holds considerable information relevant to national security. There is a direct access agreement between NZSIS and Customs that enables NZSIS to access information about border crossings, goods and craft that has been collected in connection with the performance or exercise of a function, duty or power under the Customs and Excise Act 2018. NZSIS may request assistance from Customs under s 51 of the ISA. Customs provides support to the NZSIS by providing proactive notification of events or incidents of national security interest at the border, which may include information they have collected during routine and targeted interactions with passengers and goods.

Intelligence

3.62. Customs' intelligence and assessment capability is not referred to in the Customs and Excise Act. In practice, Customs intelligence and assessment is produced to support Customs operations under the Act and other relevant legislation. As with Police, the production of intelligence and assessment is shaped by the requirements of a range of legislation, including the Customs and Excise Act, the Evidence Act and the Criminal Procedure Act (again, intelligence must be actionable and able to be used in court). This means that intelligence and assessment is generally produced at a restricted level, although Customs personnel can access all levels of classified information.

3.63. In practice, the Customs' intelligence function is led by the Manager Intelligence, who reports to the Group Manager Intelligence, Investigations and Enforcement and leads a group of around 70 intelligence personnel. Intelligence personnel produce a mix of strategic, operational and tactical intelligence and assessment, drawing on their own material, foreign partner material and material from the NAB and the Agencies. The Customs' intelligence function includes dedicated capabilities related to counterterrorism and transnational crime. In addition, Customs hosts a new Joint Border Analytics Team, which brings together Customs, Immigration New Zealand and MPI and is made up of data specialists able to provide support to the intelligence function of Customs and other agencies.[132]

3.64. Since 2017, Customs has embedded an intelligence analyst within the GCSB under s 51 of the ISA, which deals with requests by the Agencies for assistance to give effect to authorisations.

Ministry of Business, Innovation and Employment

3.65. MBIE has a broad mandate, ranging from the regulatory systems governing New Zealand markets, labour market policy and New Zealand's immigration system.

3.66. MBIE is legislative administrator for 119 Acts, with some, such as the Immigration Act 2009 setting out functions related to national security and intelligence.

3.67. The Immigration Act establishes an immigration system that, amongst other things, allows for the management of people crossing the border. One of Immigration New Zealand's main functions is to manage the entry of people who are not New Zealand citizens who wish to visit, work, study or live in New Zealand. This involves collecting and sharing information to determine individuals' compliance with their obligations under the immigration system, make decisions regarding the grant of a visa or entry permission and deport people who are not New Zealand citizens and fail to comply with immigration requirements, commit criminal offences or are considered to pose a threat or risk to security.

[132] The activities of the Joint Boarder Analytics Team do not involve the integration/aggregation of Customs, Immigration and MPI datasets – the data scientists from each agency analyse only their own agency's datasets.

3.68. MBIE is also responsible for the Outer Space and High-altitude Activities Act 2017. The purpose of this Act is to preserve New Zealand's national security and national interests when the Minister responsible for the administration of the Act is deciding whether to grant space launch licenses and payload (satellites) permits, for launches from New Zealand or by New Zealanders overseas. The Act requires the Minister to consult with security Ministers when making relevant decisions.

3.69. MBIE also hosts the Computer Emergency Response Team (CERT NZ), which works with the Agencies in relation to information assurance and cyber security. Although a cyber-security function of government, CERT NZ is not referred to in the ISA and does not have a statutory basis.

Intelligence

3.70. MBIE's intelligence and assessment functions are not referred to in its legislation. In practice, much of MBIE intelligence's outputs are produced to support MBIE operations under the Immigration Act 2009 and other relevant legislation. However, some of its intelligence reporting is provided to the whole of government and foreign partners.

3.71. MBIE has recently established a specific intelligence capability to focus on national security and intelligence. This supports a range of MBIE's activities in the national security system but is focused mainly on immigration issues, including mass arrivals, collecting and analysing a range of information. Additionally, MBIE intelligence produces country-of-origin information, covering national security topics and themes of importance and providing tactical, operational and strategic intelligence to support regulatory systems and the wider national security system. As with Customs, MBIE's intelligence draws on its own, foreign partner and NAB and the Agencies' material.

3.72. Immigration New Zealand has a direct access agreement with the NZSIS under the ISA that enables the NZSIS to have direct access to subsets of advance passenger processing information and New Zealand Electronic Travel Authority information that Immigration New Zealand collects.

3.73. Immigration New Zealand is the lead agency responsible for preventing and responding to a maritime mass arrival. There is a range of powers under the Immigration Act to enable prevention and response to a maritime mass arrival, including the ability for an immigration officer to apply a warrant of commitment authorising the detention of the members of a mass arrival group.

Issues

3.74. Our discussions with organisations involved in the wider intelligence and national security community and our own investigations have thrown up various issues that require further consideration and resolution. Some are issues that the Royal Commission identified, such as a lack of leadership for, and coordination across, the intelligence and security community as a whole, a lack of clear allocation of responsibilities and a lack of accountability against national security priorities. We will not discuss these issues in any detail here as they have been well canvassed in the Royal Commission's report and have been, or are in the process of being, addressed elsewhere.

3.75. Rather, we will focus on two particular issues that have come out of our review. These are:

- legislative deficiencies, including gaps and the use of work-arounds
- legislative inconsistencies among different agencies.

3.76. Preliminary to this, we note it is not immediately clear why so much of New Zealand's intelligence and security sector is not directly dealt with in the ISA in some way. The ISA deals in detail with the two core intelligence and security agencies, the GCSB and the NZSIS, but mentions the other two significant intelligence and security organisations, the NZDF and the Police, only peripherally and makes no explicit mention of other significant organisations such as Customs. It mentions New Zealand's principal intelligence assessment agency, the NAB, but not in any detail; it does not mention New Zealand's other significant intelligence assessment agency, the CTAG, (the inter-agency group hosted by the NZSIS) or the function of setting New Zealand's national terrorism threat level.

3.77. One consequence is that New Zealand's overall national security system includes relatively informal arrangements or groupings that have been set up to achieve particular goals but whose effectiveness depends very much on the time and effort those involved are prepared to put into them. This may fluctuate over time with changes in priorities, resources, personnel and such like.

Legislative deficiencies

3.78. As discussed, the Defence Act 1990 makes no mention of a defence intelligence function, nor does it confer on NZDF personnel the intrusive powers to exercise such a function or provide protections for them while they do so. Although the Royal (or Crown) Prerogative is one source of authority in relation to defence matters, its precise scope in the context of an intelligence function is not well understood, and statutory recognition, such as the Radiocommunications Act 1989, is piecemeal and limited in its application. The NZDF's power to carry out unlawful activities beyond circumstances of armed conflict is at best uncertain.

3.79. As a consequence, in some situations, the NZDF can only carry out particular activities within the framework provided by the ISA. The wider New Zealand security and intelligence community may be interested in the intelligence that the NZDF can collect by way of these activities. In those cases, and where it also falls within their mandates, one of the Agencies will seek a warrant (in its own name) for the relevant activity. Once the warrant is obtained, the relevant Director-General will ask the NZDF to provide assistance in giving effect to the warrant under s 51 of the ISA. The NZDF can then provide the requested assistance by carrying out the particular activity and will have the benefit of the protections the ISA provides to those who assist the Agencies.[133] The relevant Agency can then share the intelligence collected under the warrant with the NZDF.

3.80. This arrangement has an obvious attraction to both the NZDF and the Agencies. The NZDF is empowered to do something that otherwise it may not be able to do; the Agencies effectively extend their capacity beyond what their own resources would permit, and the country may well be better off as a consequence. This arrangement may well be legitimate; but it is fair to describe it as a work-around because its structure reflects the fact that NZDF does not always have certainty of protection or immunity when performing its intelligence operations.

3.81. An important function of the Agencies is to collect intelligence and provide it to people authorised to receive it, such as the NZDF. In addition, as discussed in chapter 10, the ISA provides that it is a function of the Agencies to cooperate with the NZDF[134] and to provide advice and assistance to the NZDF for the purpose of facilitating the performance or exercise of the NZDF's functions, duties or powers.[135]

---

[133] Intelligence and Security Act 2017, s 51(4).

[134] Section 13(1)(a).

[135] Section 13(1)(b).

3.82. However, there are several limitations on this latter provision, most relevantly that the Agencies are only permitted to provide advice or assistance to the NZDF in relation to functions, powers or duties that the NZDF is lawfully authorised to perform.

3.83. In the absence of specific statutory authorisation of some defence intelligence work in the Defence Act or authority under the Prerogative such as in situations of armed conflict, there is a question as to what type of assistance the Agencies can lawfully provide to the NZDF, either under their general function to cooperate with the NZDF, through "advice and assistance" under s 13(1)(b), or by way of other mechanisms. Any doubt could be removed by appropriate recognition in the Defence Act of the NZDF's intelligence function.

3.84. In 2022 the Ministry of Defence commenced a policy and legislation review that includes consideration of this issue and intends to provide the Minister of Defence with detailed advice and recommendations by the end of 2023.

3.85. A further issue is that NZDI is not defined in the ISA as an intelligence and security agency, although in practice it is described as one of New Zealand's four intelligence and security agencies.[136] We were told that this causes problems in the national security system because agencies such as Customs cannot share personal information relevant to national security directly with NZDI. This is because principle 11(g) of the Privacy Act 2020 states that personal information can only be shared if the receiving agency is an intelligence and security agency.

3.86. This is an aspect that may need further consideration in the context of the review of the Defence Act and/or the ISA and may be relevant to other agencies, such as Customs and Immigration New Zealand.

3.87. Despite being a member of the Security and Intelligence Board, Customs is also not defined as an intelligence and security agency, does not have a national security purpose and can face gaps and restrictions on sharing information relevant to national security with other agencies. As noted above, Customs has extensive powers to obtain detailed information about people and goods crossing (or seeking to cross) the border, and there is a direct access agreement between Customs and NZSIS. But, outside this regime, the sharing of certain information is restricted under the Customs and Excise Act, in particular, sharing information that Customs gathers from people at the border.

3.88. Customs may only copy documents (and then share them) if they have reasonable cause to believe that the documents amount to evidence of the commission of an offence under the Customs and Excise Act.[137] Customs must also take all reasonable steps to protect the information from being unlawfully used or disclosed beyond Customs.[138] There are further restrictions on holding or storing personal information.[139] If Customs identifies a person at the border who may pose a national security risk, they can detain the person to enable the attendance of another agency for up to four hours. Customs provides 24/7 support to the NZSIS, proactively notifying them of any events or incidents of national security interest at the border, though in some cases, they may not be able to share the reasons for notification.

---

[136] Department of the Prime Minister and Cabinet *Securing our Nation's Safety: How New Zealand manages its security and intelligence agencies* (December 2000) at [27]–[28].

[137] Customs and Excise Act 2018, s 257.

[138] Section 301.

[139] Section 301(5).

3.89. Other agencies also face restrictions on sharing information relevant to national security due to the lack of an appropriate statutory basis in the ISA or in other legislation. Other situations brought to our attention are highlighted in chapter 10.

Legislative inconsistency

3.90. One example of legislative inconsistency relates to undercover operations. The ISA contains a detailed regime covering covert activities by the GCSB and the NZSIS, including assumed personal identities,[140] corporate identities[141] and keeping a register of both.[142] By contrast, there is no such statutory regime covering Police use of undercover operations. Although there are legislative provisions that recognise that the Police do conduct such operations[143] and there are provisions they can use to help create false identities,[144] there is no comprehensive statutory scheme of the type that applies to covert activities by employees of the Agencies. The courts do review some Police undercover operations if they are relevant to the issues in particular cases,[145] but they cannot realistically provide a comprehensive regulatory regime for Police undercover operations.

3.91. The Law Commission and the Ministry of Justice considered this issue in their 2017 review of the Search and Surveillance Act 2012.[146] That review recommended that the Search and Surveillance Act be amended to include a 'covert operations' regime for Police similar to that in the ISA for the Agencies.[147] As far as we are aware, that recommendation has not yet been acted upon.

3.92. A further example is one raised by the Agencies. From time to time, NZSIS personnel may wish to log in to, say, an online chat room under an assumed name to see what is happening within it. This may arise as a real-time reaction to what they are seeing online. Before they do so, however, they must go through the assumed identity process set out in the ISA. That process may be more onerous and time consuming than is warranted in the circumstances, and the time-sensitive opportunity may be lost.[148] By contrast, other government personnel operating in areas such as immigration or investigating child exploitation material may adopt false online persona without having to go through any statutory process. These other departments are, however, subject to the collection principles under the Privacy Act, in particular Information Privacy Principle 4, relating to the manner of collecting personal information.[149]

---

140 Intelligence and Security Act 2017, ss 21–32.

141 Sections 33–44.

142 Section 45.

143 See Evidence Act 2006, ss 64, 108, 109, 120.

144 Most notably, the Births, Deaths, Marriages and Relationships Registration Act 1995, s 65, which enables the Minister of Police to apply to the Minister of Internal Affairs for false documentation in relation to birth, death, marriage/relationship and name change on behalf of undercover Police officers.

145 See, for example, *R v Kumar* [2015] NZSC 124, [2016] 1 NZLR 204; *R v Wichman* [2015] NZSC 198, [2016] 1 NZLR 753.

146 Law Commission and the Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC R141, June 2017).

147 Recommendation 64.

148 As we understand it, one way of getting round this problem is to have a number of false persona set up and ready to go when required.

149 The NZSIS and the GCSB are exempt from Information Privacy Principle 4(b) by virtue of s 28 of the Privacy Act 2020.

3.93. While not challenging the need for the assumed identity regime generally, the NZSIS has asked whether there is any real justification for using the statutory process where false identities are assumed for a short time with no interactions with other users and in circumstances of immediacy. While we see some merit in the NZSIS's point, we believe the question warrants a comprehensive study of what is occurring across government departments in relation to the use of online false identities to develop a comprehensive approach, reflecting all relevant interests.

RECOMMENDATION 01

To assist in the effective implementation of the Intelligence and Security Act 2017 (ISA), a coherent and consistent approach should be adopted in legislation governing the wider intelligence and security community. Consideration should be given to addressing legislative gaps and inconsistencies across the legislation governing the wider intelligence and security community, especially where the legislation hinders effective cooperation among New Zealand's intelligence community and the legislative frameworks applying to similar activities undertaken by different agencies differ. In particular, there should be appropriate statutory recognition for the intelligence and security functions within the New Zealand Defence Force and the New Zealand Police, especially in light of section 13 of the ISA.

CHAPTER 04
Constraints: An overview

Introduction

4.1. In this chapter we outline the constraints that the Intelligence and Security Act 2017 (ISA) places on the two intelligence and security agencies (the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS), referred to as 'the Agencies'). While we discuss the main oversight mechanisms in more detail in chapter 12, it is important to view these mechanisms in their overall context.

4.2. By constraints, we mean limitations on the Agencies' freedom of action, which include the oversight mechanisms in the ISA but also other controls, such as legislative restrictions. Reflecting the extent of the constraints, this chapter outlines the Agencies' controls and safeguards under six headings: legislative controls; internal administrative controls; Executive oversight; judicial or quasi-judicial oversight; oversight by an independent officer or agency; and parliamentary oversight.

4.3. It is important to note the constraints referred to in this chapter operate at different points in the process. Some (such as legislative requirements) operate as the Agencies are undertaking their work and attempt to control how they go about that work. The Commissioners of Intelligence Warrants are an example of officeholders whose decisions control the actions of the Agencies, for example, when they refuse or grant warrants. Other constraints operate after the fact and review actions that the Agencies have already undertaken. The Inspector-General of Intelligence and Security (Inspector-General) is an officeholder who conducts 'after-the-fact' reviews. Of course, such reviews may seek to change the conduct of the Agencies for the future.

4.4. An initial point to note is that the ISA is unusual because it is unlikely that its terms will be the subject of interpretation by the courts (although that is not impossible).[150] Judicial proceedings involving the interpretation of provisions within the ISA are unlikely to be brought. This is partly because of the secrecy surrounding the Agencies' activities, so affected parties will not be aware of the issues of interpretation, and partly because any disputes as to interpretation are likely to be between entities within the public sector (for example, an Agency and the Inspector-General) and these are likely to be addressed in other ways. The Agency may seek an opinion from the Solicitor-General. As far as the Agency is concerned, that opinion will be directive. It will not bind the Inspector-General, however, given the Inspector-General's status as an independent statutory officer. Although the Solicitor-General's opinion will be directive from their perspective, the Agencies should nevertheless respect the Inspector-General's interpretation

[150] For example, in *Attorney-General v Dotcom* [2013] NZCA 43, [2013] 2 NZLR 213, the Crown accepted that the GCSB had acted illegally and that Mr Dotcom was entitled to a declaration to that effect and to compensation: at [26].

of the law given the Inspector-General's important, independent and expert oversight function. Whether this position is satisfactory is an issue addressed in chapter 12 where we discuss the position of the Inspector-General.

Legislative controls

4.5. Legislation governing intelligence and security agencies in democracies imposes legislative controls and constraints on them through its terms. So, the ISA sets out the objectives, functions, duties and powers of the Agencies. Legislative provisions dealing with such matters set the framework within which the Agencies are intended to act. We give two illustrations.

4.6. First, there are five sections early in the ISA that set a general framework for the Agencies' performance of their functions, as follows.

- Section 16 provides that the Agencies are not enforcement agencies, except in certain limited circumstances.
- Section 17 implements part of the s 3 purpose provision by directing that, when performing their functions, the Agencies must act: (i) consistently with New Zealand law and all human rights obligations Aotearoa New Zealand law recognises; (ii) independently and impartially in their operations; (iii) with integrity and professionalism; and (iv) in a way that facilitates effective democratic oversight.
- Section 18 requires the Directors-General of the Agencies to take all reasonable steps to ensure their Agency's activities are relevant to their functions, are free of irrelevant influences and considerations and are politically neutral, and any cooperation with foreign jurisdictions and international organisations accords with New Zealand's law and with all human rights obligations New Zealand law recognises.
- Section 19 provides that the exercise by a person or class of persons in New Zealand of their right to freedom of expression under the law (including the right to advocate, protest or dissent) does not, of itself, justify the Agencies taking any action in respect of them.
- Section 20 requires the Directors-General to consult the Leader of the Opposition regularly to keep the Leader informed about matters relating to the Agencies' functions.

These provisions are intended to constrain and guide the Agencies as they undertake their work. We recommend in this report that additions be made to these provisions.

4.7. Second, in relation to intrusive powers, we illustrate the point by reference to s 58 of the ISA. As discussed in chapter 5, 'national security' is not defined in the ISA and is a term capable of being interpreted either narrowly or broadly. Section 58 sets out the circumstances in which the Agencies are entitled to seek warrants against New Zealanders on protection of national security grounds. The specificity of s 58 narrows the potential scope of 'national security' as it applies to New Zealanders, at least to some extent. In formulating provisions of this type, the Legislature identifies what, in its view, is the appropriate extent of the Agencies' powers, or, put another way, where the appropriate boundary lies between intrusive powers and fundamental freedoms. In that way, statutory provisions reflect important policy or evaluative judgments by the Legislature. As noted, one of the matters identified in the review's terms of reference is whether the ISA "appropriately balances national, community and individual security with individual privacy and other rights".

4.8. Although legislative provisions are not self-enforcing, they can be effective as controls or constraints if the agencies whose work they govern have strong compliance cultures, supported by appropriate internal policies and procedures. But even if a strong compliance culture exists within the Agencies, effective external control and oversight mechanisms remain necessary, partly to reinforce the importance of compliance and ensure effective accountability and partly to enhance public confidence in the work of the Agencies, much of which necessarily occurs in secret.

Internal administrative controls

4.9. Like any organisation that hopes to act effectively and efficiently, in line with mandated objectives and obligations, the Agencies need to have internal policies and procedures with which their personnel must comply. This is reflected in the ISA, which explicitly expects that the Agencies will develop relevant policies and procedures. So, for example, one of the functions of the Inspector-General is to conduct periodic reviews into the effectiveness and appropriateness of:

- the Agencies' procedures to ensure compliance with the ISA's provisions concerning the issue and execution of authorisations
- the Agencies' compliance systems for operational activities, including all their supporting policies and practices relating to various specified matters, including legal compliance generally.[151]

4.10. The ISA requires that ministerial policy statements set out procedures, protections and restrictions on activities, where appropriate.[152] An example is the ministerial policy statement on "Conducting surveillance in a public place".[153] This statement requires the Agencies to actively consider principles, including key human rights considerations, which constitute a framework for good decision-making when planning and conducting surveillance in a public place. The previous version, in place from September 2017 to March 2022, was discussed by the Inspector-General in his public report on the NZSIS's use of closed-circuit television (CCTV).[154]

4.11. Legislation may well address the effect of non-compliance with an internal policy or procedure. So:

- section 29 of the ISA provides that evidence of an assumed identity may be issued, given, changed or cancelled by a Minister, statutory officer and government or private sector agency[155] without complying with any policy or practice that requires compliance with, for example, any prescribed process or procedure
- section 171 allows a person to complain to the Inspector-General that they have been adversely affected by (among other things) "any … practice, policy, or procedure of an intelligence and security agency",[156] which may permit a complaint based on non-compliance with a relevant policy or procedure.

---

[151] Intelligence and Security Act 2017, s 158(1)(f).

[152] Section 210.

[153] Ministerial Policy Statement "Conducting surveillance in a public place" (March 2022).

[154] Inspector-General of Intelligence and Security *Review of NZSIS use of closed-circuit television (CCTV)* (online, June 2021).

[155] Intelligence and Security Act 2017, s 22.

[156] Section 171(2).

4.12. In the normal course, however, the main steps to ensure compliance with internal procedures and practices are likely to occur within the Agencies themselves. They are likely to include a range of mechanisms to help ensure the development and maintenance of a compliance culture within each Agency, such as induction processes, refreshers, checklists, sign off and reporting requirements, periodic audits and performance evaluations, and so on. So, for example, the 2021 NZSIS Annual Report says:[157]

> We have a responsibility to ensure that we use our powers and access in a manner that is lawful, necessary, and proportionate. To ensure that our staff use our powers in this way, the NZSIS has a compliance framework and runs a regular programme of audits and reviews. We encourage a culture of self-reporting of compliance incidents, which are reported to the Inspector-General of Intelligence and Security (IGIS). These incidents often highlight improvements required to systems and processes, which are then addressed. The NZSIS Compliance team manages a compliance training framework that ensures all staff receive training on their compliance obligations every year.

4.13. The impression we have gained from our interactions with the Agencies is that they currently have reasonably strong compliance cultures.

Executive oversight

4.14. The Executive oversight we are concerned with is that carried out by relevant Ministers.[158] Currently, two Ministers are relevant. First, the Prime Minister as the Minister for National Security and Intelligence has responsibility for the national security system as a whole. Second, the Hon Andrew Little is the Minister Responsible for the GCSB and the NZSIS. He is responsible for setting the direction and priorities of the Agencies and for the performance of several important functions under the ISA. They include the issue of warrants authorising the Agencies to carry out activities that would otherwise be unlawful, where he acts either alone or in conjunction with a Commissioner of Intelligence Warrants depending on the circumstances. That responsibility will give the Minister an insight into the Agencies' day-to-day operations. As noted in chapter 3, both Ministers are supported in their national security roles by the Department of the Prime Minister and Cabinet.

4.15. One important function of the Minister Responsible for the Agencies is to issue ministerial policy statements with guidance for the Agencies on various matters, for example: assumed identities; surveillance in public places; use of publicly available information; and cooperation with overseas public authorities.[159] The National Security Group within the Department of the Prime Minister and Cabinet develops the statements for the Minister. They are significant because they cover activities that are lawful (and therefore do not need a warrant) but that may involve elements of deception or intrusion and other areas where ministerial guidance was considered appropriate. According to the select committee that considered the New Zealand Intelligence and Security Bill, the statements would "provide clarity, oversight and accountability, transparency, and public confidence and reassurance".[160]

---

[157] NZSIS *Annual Report 2021* (2021) at 71.

[158] The Inspector-General of Intelligence and Security is an independent statutory officer and so is not part of the Executive.

[159] Intelligence and Security Act 2017, ss 206–207.

[160] Foreign Affairs, Defence and Trade Committee *New Zealand Intelligence and Security Bill* (24 February 2017) at 11.

4.16. To facilitate this:

- Section 209 of the ISA requires the Directors-General of the Agencies and their employees to "have regard to" any relevant ministerial policy statement when making decisions or taking action. In addition, other agencies may also be required to "have regard to" relevant ministerial policy statements. For example, where an employee of an Agency wishes to acquire an assumed identity and requests another agency[161] for help, s 26(3)(b) requires that other agency to have regard to any relevant ministerial policy statement (to the extent it knows about it).
- When carrying out an inquiry or a review, the Inspector-General must have regard to any relevant ministerial policy statement and the extent to which the relevant agency had regard to it.[162] Examples of references to ministerial policy statements are found in the reports issued by the Inspector-General in relation to an NZSIS warning[163] and the review of activity and assessments under the Outer Space and High-altitude Activities Act 2017.[164]
- The Directors-General must publish ministerial policy statements, but not any information in them that may prejudice the Agencies' operations or New Zealand's interests.[165]

4.17. Like other Ministers, the Prime Minister and Minister Responsible for the Agencies are answerable to Parliament, and ultimately to the public, for the conduct of their portfolios. However, the scope is limited for meaningful parliamentary scrutiny of the work of the Agencies, given much of it is conducted in secret and much of the information they deal with is classified. Despite this, members of Parliament have taken the opportunity to question Ministers in the House on intelligence matters, as shown in the examples below.

- On 3 August 2020, Golriz Ghahraman asked: "How many warrants allowing the SIS [Security Intelligence Service] to conduct surveillance or intercept communications of any Members of Parliament, if any, has the Minister signed, listed by name of MP [member of Parliament], Party and date the warrant was signed?"[166]
- On 8 February 2022, Paul Goldsmith asked: "How much expenditure, if anything, has been spent to date of the $0.564 million allocated to the 'Office Inspector-General of Intelligence and Security' in Budget 2020; of any such expenditure, what is the most detailed available breakdown of what it has purchased?"[167]

In addition, the members of the Intelligence and Security Committee can question the Agencies in their public and private meetings.

---

[161] Defined to include both public and private sector organisations: see Intelligence and Security Act 2017, s 22.

[162] Intelligence and Security Act 2017, s 158(2).

[163] Inspector-General of Intelligence and Security *Review of an NZSIS Warning* (online, October 2022) at 6.

[164] Inspector-General of Intelligence and Security *Report into a review of GCSB and NZSIS activity and assessments under the Outer Space and High-altitude activities Act 2017* (online, April 2021) at 6.

[165] Intelligence and Security Act 2017, s 215.

[166] Golriz Gharahrman to the Minister responsible for the NZSIS, 3 August 2020, NZWPQ 15150 (2020).

[167] Hon Paul Goldsmith to the Minister of Justice, 8 February 2022, NZWPQ 873 (2022).

Judicial or quasi-judicial oversight

4.18. In comparable jurisdictions, such as Canada, intelligence warrants are issued by sitting judicial officers. By contrast, in New Zealand, as in the United Kingdom, this function is performed by retired judges, albeit that they act in conjunction with Ministers. In Australia, some warrants are issued by sitting judges[168] and others by the Attorney-General or a Minister.[169]

4.19. At the time of the Cullen/Reddy review, there was one Commissioner of Security Warrants, who approved warrants in relation to New Zealanders. When the Commissioner was unavailable, the Attorney-General was empowered to act in the Commissioner's place. The Cullen/Reddy report considered this configuration was unsatisfactory and recommended a pool of three Commissioners be created – a Chief Commissioner and two additional Commissioners – and that the Attorney-General be removed. The report noted that the purpose of having a judicial commissioner involved was "to ensure an assessment that is impartial and independent from the executive".[170] This recommendation was accepted and is reflected in the ISA.

4.20. Accordingly, New Zealand presently has three Commissioners of Intelligence Warrants, including the Chief Commissioner. They are appointed by the Governor-General on the recommendation of the Prime Minister and must be retired High Court judges. This means that any judge who has been a member of the High Court, Court of Appeal or Supreme Court is eligible for appointment. While they have several functions, the most important relate to what the ISA refers to as Type 1 warrants, which are warrants that authorise otherwise unlawful activities for the purposes of intelligence gathering in relation to New Zealand citizens and permanent residents.

4.21. The warranting framework is discussed in more detail in chapter 7. Here we simply look at how the ISA frames the Commissioners' tasks as a preliminary to the further discussion of Commissioners in chapter 12.

4.22. In relation to Type 1 warrants, s 114(a)–(d) of the ISA identifies four functions for Commissioners:

- to **advise** the authorising Minister on applications
- to **consider** applications **with** the authorising Minister
- to **deliberate on** applications **with** the authorising Minister
- to **issue** warrants under the relevant section **jointly with** the authorising Minister.

4.23. Two important points emerge from this statutory description of the Commissioners' functions in relation to Type 1 warrants:

- first, the 'advice' function presumably reflects that the authorising Minister may need guidance as to how an application should be approached, at least initially
- second, the words used to describe the other three functions – 'consider with', 'deliberate on … with' and 'issue jointly with' – suggest that Parliament saw the Type 1 warrant-issuing process as being closely collaborative.

---

168 See, for example, Surveillance Devices Act 2004 (Australia), Part 2 – Warrants.

169 See, for example, Australian Security Intelligence Organisation Act 1979, s 26.

170 Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM *Intelligence and Security in a Free Society – Report of the First Independent Review of Intelligence and Security in New Zealand* (February 2016) at [6.88] (*Cullen/Reddy report*).

4.24. It is relevant to note that the Cullen/Reddy report had recommended that the issuing Minister for both Type 1 and Type 2 warrants be the Attorney-General.[171] The rationale was that, as the principal law officer of the Crown, the Attorney-General was the appropriate member of the Executive branch to take human rights considerations into account and to ensure the rule of law was upheld. The Attorney-General would also be able to assess whether the activity under consideration was in the national interest.[172]

4.25. This recommendation was not accepted, however, following significant debate in the select committee and subsequently. The Hon Christopher Finlayson KC, who was both Attorney-General and Minister Responsible for the Agencies at the time, considered the Attorney-General should stand back from the Agencies' day-to-day operations and that, operationally, it was better for the Minister directly involved to be the one issuing the warrants. The Labour Opposition accepted this, although saying it was an "on-balance" decision.[173] Hon David Cunliffe, who was a member of the select committee that considered the Bill, noted the risk that the Minister concerned might become too close to their department operationally and could lack "the objectivity of judgment to draw a line at exactly the right place where an intercept would not be justified because there were other lawful means, for example, of preventing the harm".[174] Mr Cunliffe said the matter should be kept under review.

4.26. We have not heard anything during our review to suggest the decision to choose the Minister rather than the Attorney-General should be revisited. This means, however, that the Commissioners' 'advice' function, and the collaborative nature of the warranting process contemplated by the ISA's provisions, may assume more or less practical importance, depending on the Minister's background and the approach they adopt to the role.

4.27. In addition to the four functions identified in paragraph [4.22], s 114 confers the following functions on Commissioners:

- to consider with the authorising Minister applications for permission to access restricted information
- to consider with the responsible Minister applications for approval to obtain business records
- to conduct reviews under s 56 of the Telecommunications (Interception Capability and Security) Act 2013 relating to significant network security risks
- to conduct reviews under s 27GF of the Passports Act 1992 relating to decisions to refuse to issue, or to cancel or retain possession of, a New Zealand travel document
- to perform any other functions conferred or imposed on Commissioners by or under the ISA or any other enactment.

4.28. Under s 115, the Chief Commissioner has additional functions. For example, the Chief Commissioner is the point of contact for all communications with the Commissioners, receives all applications for Type 1 intelligence warrants, allocates warrant applications to particular Commissioners and makes revocation decisions regarding Type 1 warrants issued on an urgent basis by the authorising Minister acting alone.

---

171 Cullen/Reddy report, at [6.28].

172 Cullen/Reddy report, at [6.73]–[6.75].

173 Hon David Cunliffe during the Third Reading of the Intelligence and Security Bill, (21 March 2017) 721 NZPD.

174 Above n.

Independent oversight: Inspector-General of Intelligence and Security

4.29. In December 1995, the then Prime Minister, Rt Hon Jim Bolger, introduced the Intelligence and Security Agencies Bill. An important objective of that Bill was to increase parliamentary and administrative oversight of the Agencies. Two relevant steps were proposed, first, the establishment of a Parliamentary Intelligence and Security Committee and second, the creation of a position of Inspector-General of Intelligence and Security to replace the Commissioner of Security Appeals and expand the oversight role.

4.30. Ultimately, both the Intelligence and Security Committee and the office of Inspector-General of Intelligence and Security were established under their own individual statutes. The object of the Inspector-General of Intelligence and Security Act 1996 was described in s 4 as follows:

> The object of this Act is to provide for the appointment of an Inspector-General who will assist each Minister who is responsible for an intelligence and security agency in the oversight and review of that intelligence and security agency and who will, in particular,—
>
> (a) assist the Minister to ensure that the activities of that intelligence and security agency comply with the law; and
>
> (b) ensure that complaints relating to that intelligence and security agency are independently investigated.

The Act required that the Inspector-General be a retired High Court judge.

4.31. An interesting feature of the s 4 purpose statement is that the role of the Inspector-General was described as assisting the responsible Minister(s) in the oversight and review of the Agencies. To facilitate this, the Inspector-General was required, following an inquiry, to report to the Minister and Director-General of the relevant Agency.

4.32. In 2013, the government decided to make several important changes to the legislative framework governing the Agencies, including the office of Inspector-General. In May 2013, the Hon Judith Collins introduced the Government Communications Security Bureau and Related Legislation Amendment Bill on behalf of the Prime Minister, Rt Hon John Key. In relation to the changes to the Inspector-General's position, Hon Judith Collins said:[175]

> In broad terms, the changes to strengthen the Inspector-General legislation fall into three categories: the first is legislative changes, expanding the Inspector-General of Intelligence and Security's work programme, and enhancing reporting responsibilities; secondly, increased resourcing of the Office of the Inspector-General of Intelligence and Security; and, thirdly, legislative change to address the required qualification to broaden the pool of candidates and the appointment process. It is the Government's intention that the Inspector-General's office will become a more proactive overseer of the intelligence community that is able to launch its own investigations and is better resourced to do so.

[175] Hon Judith Collins during the First Reading of the Government Communications Security Bureau and Related Legislation Amendment Bill, (8 May 2013) 689 NZPD.

4.33. We will not discuss the detail of the changes. We simply note that:

- the previous requirement that the Inspector-General be a retired High Court judge was removed
- the role of Deputy Inspector-General was established
- a requirement that the Inspector-General's reports be made publicly available was introduced
- provision was made for the appointment of a two-person advisory panel to advise the Inspector-General, either on their own initiative or following a request from the Inspector-General.
- the Inspector-General's ability to act independently was enhanced.

4.34. This brings us to the provisions in the ISA dealing with the Inspector-General. Part 6 deals with oversight of the Agencies. Section 156 sets out the purpose of Part 6. Given its importance to the discussion that follows in this chapter and later in chapter 12, we set it out in full below.

> **Purpose of Part**
>
> (1) The purpose of this Part is to provide for the independent oversight of intelligence and security agencies to ensure that those agencies act with propriety and operate lawfully and effectively.
>
> (2) To achieve this purpose,—
>
> (a) the office of the Inspector-General of Intelligence and Security is continued, with the Inspector-General having the functions, duties, and powers to—
>
> (i) ensure that the intelligence and security agencies conduct their activities lawfully and with propriety; and
>
> (ii) ensure that complaints relating to the intelligence and security agencies are independently investigated; and
>
> (iii) advise the New Zealand Government and the Intelligence and Security Committee on matters relating to the oversight of the agencies:
>
> (b) the Intelligence and Security Committee is continued to provide parliamentary scrutiny of the policies, administration, and expenditure of the intelligence and security agencies.

4.35. Two features of s 156(1) should be noted.

- First, the objective of the Part is to provide for **independent** oversight of the Agencies.
- Second, the purpose of that independent oversight is to **ensure** that the Agencies:
  - act **with propriety**
  - operate **lawfully**
  - operate **effectively**.

4.36. Section 156(2)(a) goes on to identify the three main functions of the Inspector-General within the oversight structure:

- to ensure that the Agencies conduct their activities "lawfully and with propriety"
- to ensure that complaints relating to the Agencies are independently investigated
- to advise the government and the Intelligence and Security Committee on matters relating to the oversight of the Agencies.

It is, accordingly, not part of the Inspector-General's functions to ensure the Agencies operate effectively, other than to review the effectiveness and appropriateness of the Agencies' compliance procedures and systems[176] and to report annually on the extent to which the Agencies' compliance systems are "sound".[177]

4.37. An important feature of ss 156(1) and 156(2)(a) is that they distinguish between the legality and propriety of an Agency's activities. This distinction is carried through into s 158, which sets out the Inspector-General's functions. Under s 158(1)(a), the Inspector-General may carry out an inquiry into an Agency's compliance with New Zealand law, including human rights law; under s 158(1)(c), the Inspector-General may conduct an inquiry into the propriety of particular activities of the Agencies.

4.38. Parliament has accepted, then, that an Agency may act in a way that is lawful but, when viewed from the perspective of morality or social acceptability, is improper. This 'propriety' qualification[178] becomes relevant, for example, when considering issues such as whether the Agencies should be entitled to access information that is in the public domain only because it has been unlawfully hacked from a private database.

4.39. Under the ISA, the Inspector-General is empowered to carry out inquiries and reviews (including complaint investigations). To perform these functions the Inspector-General has a right of access to Agency records.[179] In relation to inquiries, the Inspector-General has several important powers, for example, the power to summons people and require them to give evidence on oath. At the conclusion of an inquiry, the Inspector-General must write a report and send it to the Minister and the Director-General of the relevant Agency, and to the Prime Minister or the Intelligence and Security Committee if either has asked for the inquiry. Reports must be made public, subject to a prohibition on publishing information that may prejudice New Zealand's security or defence or international relations. Although the Minister must respond to the report, the relevant Agency has no express statutory obligation to respond, or to implement any recommendations in the report. The Inspector-General may, however, raise with the Minister the issue of the Agency's compliance with the recommendations.

4.40. By contrast, when conducting a review, the Inspector-General lacks the explicit coercive powers available during an inquiry. However, the following considerations mean the Agencies must still cooperate with reviews.

---

[176] Intelligence and Security Act 2017, s 158(1)(f)(i).

[177] Section 222(2)(c).

[178] 'Propriety' is not defined in the Intelligence and Security Act 2017, but as described previously by the Inspector-General, "it goes beyond specific questions of legality; for example, whether the agency acted in a way that a fully informed and objective observer would consider appropriate and justifiable in the particular circumstances". Inspector-General of Intelligence and Security *Annual Report 2015* (online, October 2015) at 20.

[179] Intelligence and Security Act 2017, s 217.

- First, there are some reviews that the Inspector-General is obliged to conduct.[180] Obviously, these cannot be undertaken without the cooperation of the Agencies, so there is at least an implicit obligation that they cooperate.
- Second, even in the absence of a mandatory obligation to conduct a review, the Inspector-General cannot be prevented from performing their statutory functions by non-cooperation on the part of the Agencies. It is an offence under ISA to obstruct, hinder or resist the Inspector-General in the exercise of their powers, or to refuse or wilfully fail to comply with a lawful requirement of the Inspector-General.[181] The Agencies also have a general duty to act in a manner that facilitates effective democratic oversight.[182] The Inspector-General is one component of effective democratic oversight, so that the Agencies are obliged to facilitate their work. This means the Agencies are obliged to cooperate.

4.41. Two important areas of review for the Inspector-General are the issue of warrants and the way warranted activities are carried out.[183] But any irregularity the Inspector-General identifies in a review does not affect the validity of a warrant or any activity carried out under it.[184]

4.42. Finally, we note that s 161 provides for interactions between the Inspector-General and other oversight bodies.

- Under s 161(1), the Inspector-General must have regard to the functions of the Auditor-General in relation to the Agencies and may consult the Auditor-General to avoid both officials conducting inquiries into the same matter.
- Under s 161(2), the Inspector-General may consult with the Auditor-General, an Ombudsman, the Privacy Commissioner, a Human Rights Commissioner, the Independent Police Conduct Authority and the State Services Commissioner and may provide them with any necessary information.

Corresponding consultation provisions are included in legislation governing the Ombudsmen[185] and the Privacy Commissioner.[186]

4.43. We discuss the issue of consultation between the various oversight agencies in chapter 12.

Parliamentary oversight

4.44. In this section, we describe two mechanisms of parliamentary oversight: the Intelligence and Security Committee and the Controller and Auditor-General.

Intelligence and Security Committee

4.45. Much of Mr Bolger's speech when introducing the Intelligence and Security Agencies Bill in December 1995 concerned the proposed Intelligence and Security Committee. Having outlined concerns about the need for greater oversight of the Agencies, Mr Bolger said:[187]

[180] An example is 12 monthly reviews into certain compliance procedures: section 158(1)(f).
[181] Section 225.
[182] Section 17(d).
[183] Intelligence and Security Act 2017, s 158(i).
[184] Section 163.
[185] Ombudsmen Act 1975, s 21C.
[186] Privacy Act 2020, s 208(1)(c).
[187] Rt Hon Jim Bolger during the First Reading of the Intelligence and Security Agencies Bill, (19 December 1995) 552 NZPD.

> It is against this background that the Bill proposes the establishment of a special committee of parliamentarians to perform the functions in relation to the New Zealand Security Intelligence Service and the Government Communications Security Bureau that, in the case of other Government departments, are performed by a parliamentary select committee … The Intelligence and Security Committee of parliamentarians will comprise senior members of Parliament, including the Prime Minister and the Leader of the Opposition. Parliament will be invited to endorse the nominations for committee membership …
>
> The committee will deal with sensitive issues that impinge upon national interests and will often handle highly classified information. It is appropriate in this situation that membership of the committee should be at a senior level.

4.46. Mr Bolger then described how the proposal for the Committee had been developed. He said:

> In developing the proposal for the establishment of the committee, close attention has been paid to the practice adopted by like Governments overseas. It is significant that in both Australia and Britain parliamentary oversight committees for intelligence and security agencies have been established by legislation. The British Intelligence Services Act provided, for the first time in the United Kingdom, a means by which the British intelligence and security services could be made accountable to Parliament. In its functions, the committee will not be dissimilar to the normal parliamentary select committees. Under the relevant Standing Orders, the committee will deal with matters of policy, finance, and administration of the intelligence and security agencies, reviewing their estimates, monitoring their financial performance, and receiving their annual reports. The committee will report to Parliament. The establishment of this committee is an important measure that will achieve in a manner appropriate to the intelligence and security agencies proper oversight, review, and accountability, the absence of which has been of concern to members of this House.

4.47. Three features of the United Kingdom legislation to which Mr Bolger referred, the Intelligence Services Act 1994, are worth noting. First, the Chair and members of the United Kingdom committee were appointed by the Prime Minister after consultation with the Leader of the Opposition – Parliament played no part in the process. Second, Ministers were not eligible for appointment to the United Kingdom committee. Third, the United Kingdom committee's function was "to examine the expenditure, administration and policy" of three intelligence and security agencies: MI5, MI6 and GCHQ.

4.48. The long title to the New Zealand Act, the Intelligence and Security Committee Act 1996, indicates the Act was intended "to increase the level of oversight and review of intelligence and security agencies by establishing an intelligence and security committee". The functions of the Committee were to examine the Agencies' "policy, administration and expenditure"; to receive and consider the Agencies' annual reports; to consider intelligence and security related matters referred to the Committee by Parliament, and matters referred by the Prime Minister. However, these functions were subject to several limitations, most particularly that the Committee was not permitted to inquire into anything that was "operationally sensitive", which was broadly defined.

4.49. The Committee comprised five members:

- the Prime Minister
- the Leader of the Opposition

- two members of the House nominated by the Prime Minister after consulting the leader of each party in government
- one member of the House nominated by the Leader of the Opposition, with the agreement of the Prime Minister, after consultation with the leader of each party not in government or in coalition with a government party.

The nominees were put to the House for endorsement. If the House refused to endorse a member, another nomination was made in accordance with the relevant process.

4.50. The Prime Minister chaired the Committee. The 1996 Act said "for the avoidance of doubt" that, when performing the Committee's functions, a member of the Committee acted in their official capacity as a member of Parliament. Presumably this was considered necessary because the Committee was a statutory rather than select committee.

4.51. Three relevant points emerge.

- First, Mr Bolger made it clear that the government had looked closely at developments in comparable jurisdictions and sought to bring New Zealand's oversight arrangements into line with theirs.
- Second, members of the Executive, in particular the Prime Minister, were members of the Committee and exercised significant control over both its membership and its operations. In this respect, the Committee was not comparable to a typical select committee, nor could it fairly be described as an 'independent' oversight mechanism given the Prime Minister's responsibility for the country's national security.
- Finally, the Committee's power to inquire into the Agencies' activities was significantly limited.

4.52. Little change occurred to the legislative provisions governing the Intelligence and Security Committee in the 2013 reforms. However, as discussed in chapter 1, provisions dealing with the periodic review process were introduced into the Intelligence and Security Committee Act 1996 at this time. They were carried through into the ISA largely unchanged. Under s 236(3)(a) of the ISA, the terms of reference for a periodic review must be specified by the Prime Minister and "may include any matter relevant to the functions, effectiveness, and efficiency of the intelligence and security agencies and their contribution to national security".[188] The significance of this is discussed at paragraph [4.58] and [4.67] and following.

4.53. A feature of the debates in the House concerning the 2013 reforms was the criticism made of the Intelligence and Security Committee. For example, Hon David Shearer, then Leader of the Opposition, said that its ability to provide oversight was "woeful";[189] Hon Phil Goff, also a member of the Committee for three years, described it as a "farce";[190] similarly, Dr Russel Norman, Co-leader of the Greens and member of the Committee, said there was no parliamentary oversight of the Agencies and pointed to the Committee's lack of powers.[191]

---

[188] Intelligence and Security Act 2017, s 236(3)(a).

[189] Hon David Shearer during the First Reading of the Government Communications Security Bureau and Related Legislation Amendment Bill, (8 May 2013) 689 NZPD.

[190] Hon Phil Goff during the First Reading of the Government Communications Security Bureau and Related Legislation Amendment Bill, (8 May 2013) 689 NZPD.

[191] Dr Russel Norman during the First Reading of the Government Communications Security Bureau and Related Legislation Amendment Bill, (8 May 2013) 689 NZPD.

4.54. One topic of debate as the New Zealand Intelligence and Security Bill (which became the ISA) went through the House in 2016/17 was the size and composition of the Intelligence and Security Committee. Green and Labour members argued several deficiencies existed with the Committee's structure, for example, the fact it was chaired by the Prime Minister, who was responsible for national security and intelligence issues generally,[192] and the limited representation of minor parties.[193]

4.55. The government responded to some of these concerns, at least to the extent that the ISA made provision for additional members. The Committee's membership was raised from five to a minimum of five and a maximum of seven, the precise number to be determined by the Prime Minister in consultation with the Leader of the Opposition.[194] The ISA sets out the process by which the Prime Minister and the Leader of the Opposition are to identify the nominees to be put to the House of Representatives for endorsement.[195] The Prime Minister must make the nominations "as soon as practicable after the commencement of each Parliament".[196]

4.56. Under s 193 of the ISA, the functions of the Committee include examining the Agencies' "policy, administration and expenditure"; receiving and considering the Agencies' annual reports; conducting an annual review of each Agency after receiving their respective annual reports; considering matters referred to the Committee by Parliament; and requesting the Inspector-General to conduct an inquiry into issues relating to the Agencies' compliance with the law and the propriety of their activities. The Public Finance Act 1989 sets what the Agencies must provide to the Intelligence and Security Committee as part of its Estimates and Supplementary Estimates examination. Further, s 39 of the Public Finance Act 1989 requires the responsible Minister to forward a copy of the Agencies' strategic intentions to the Committee.

4.57. The Committee may not, however, inquire into any matter within the Inspector-General's jurisdiction, any matter that is operationally sensitive or any complaint that can be resolved under any other statute. While 'operationally sensitive' is not defined, the breadth and significance of the term is plain from what it includes: "including any matter that relates to intelligence collection and production methods, or sources of information".[197] Issues relating to intelligence collection will often raise important issues of policy, which might be expected to fall within the jurisdiction of a democratic oversight body.

4.58. It is noteworthy that the functions of the Intelligence and Security Committee do not refer explicitly to assessing the operational effectiveness of the Agencies. Apart from the mention of effectiveness in the purpose statement for the oversight provisions in s 156(1), no reference is made to assessing the Agencies' general effectiveness anywhere in Part 6, the only mention is in the periodic review provisions in s 236(3)(a) of Part 7.

---

[192] See, for example, Hon David Shearer during the First Reading of the New Zealand Intelligence and Security Bill, (18 August 2016) 716 NZPD; Hon Grant Robertson during the Second Reading of the New Zealand Intelligence and Security Bill, (9 March 2017) 720 NZPD.

[193] See, for example, Hon Metiria Turei during the First Reading of the New Zealand Intelligence and Security Bill, (18 August 2016) 716 NZPD.

[194] Intelligence and Security Act 2017, s 194(1).

[195] Sections 194 and 196.

[196] Section 196(1).

[197] Section 193.

4.59. The Committee must meet in private except when conducting its annual review of an Agency following receipt of the Agency's annual report or if the Committee unanimously agrees that the Committee should meet in public.[198]

4.60. There seems to be nothing to prevent the Committee from holding inquiries, as long as they relate to its functions. In terms of access to oral and documentary evidence, the following apply.

- The Director-General of an Agency must appear before the Committee at the Committee's request.[199]
- The Committee may request others to attend and give evidence or to produce relevant documents and other information.[200]
- Where the Committee asks anyone to produce relevant documents or other information, the person must either arrange for the document or information to be made available or inform the Committee that the material falls within the definition of 'sensitive information' in s 202 of the ISA.[201] 'Sensitive information' may be disclosed to the Committee if the custodian of the material considers it 'safe' to disclose it, or if the Prime Minister considers that disclosure is in the public interest.[202]

Controller and Auditor-General

4.61. Recommendation 5 in the report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019 (the Royal Commission) deals with the Auditor-General's role in relation to the Agencies.[203] The Controller and Auditor-General is an officer of Parliament who helps Parliament to perform its role of holding the Executive accountable by undertaking audit and similar activities. Relevantly:

- Under the Public Finance Act 1989, the Auditor-General audits an organisation's 'performance information' against the relevant appropriation as part of its end of year financial audit.
- Under the Public Audit Act 2001, the Auditor-General can conduct 'performance audits'.

4.62. At the end of the financial year, the Directors-General must provide an annual report to the responsible Minister. This report must contain the information required by s 45 of the Public Finance Act 1989 and certain other information set out in the ISA, including financial statements for the appropriations they administer. The information required by s 45 also includes, for example, an assessment of the Agency's progress in relation to its strategic intentions. In practice, the Agencies produce a classified and an unclassified annual report, with most information about the Agencies' achievement of performance measures contained in the classified report.

---

[198] Schedule 3, cl 22.

[199] Section 201(1).

[200] Section 201(2).

[201] The definition of "sensitive information" in s 202(1) of the Intelligence and Security Act 2017 uses the same language as used in s 6(a)–(d) of the Official Information Act 1982.

[202] Intelligence and Security Act 2017, s 203.

[203] Royal Commission of Inquiry *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020).

4.63. As we understand it, the essential position is that the Auditor-General does not conduct an audit of the performance information of the GCSB and NZSIS under Public Finance Act 1989. Several sections in the Act provide that some of its requirements do not apply to the Agencies, for example, ss 15A(4)(a) and s 45E, in order to maintain the security of classified information. This differs from other public entities where this information is required to be audited.

4.64. Nevertheless, the Auditor-General may provide a written and supporting oral briefing to the Intelligence and Security Committee as part the annual review process. This briefing may summarise the audit findings and provide comment on any significant matters the Auditor-General wishes to raise relating to aspects of Agencies' performance, which could include commenting on the adequacy of the performance measures. The Auditor-General may also provide a written and supporting oral briefing for the Committee regarding Budget Estimates for the Agencies each year. These briefings contain suggestions for questions the Committee may wish to ask of the Agencies as part of the Committee's oversight role.

4.65. Furthermore, the Auditor-General can carry out performance audits of the Agencies under the Public Audit Act 2001. We know of three:

- in 2003, relating to managing threats to New Zealand's domestic security[204]
- in 2016, relating to governance of the national security system[205]
- in 2017, relating to border security and the use of information to process passengers.[206]

We understand the Auditor-General has a performance audit on cybersecurity on his 2022/23 annual plan that will involve scrutiny of the GCSB.

4.66. These performance audits were useful because they identified areas for further work. For example, the 2003 audit identified the need for development of a whole-of-government domestic security strategy and greater coordination between agencies involved in domestic intelligence collection. The 2017 border security audit drew attention to difficulties in information sharing resulting from outdated or incompatible legislation governing the border security agencies and the need for clearer accountabilities. It identified the need for strategy for reducing information-sharing barriers. It is not clear what follow up has occurred of these findings. The points made by the Auditor-General in his 2003 report about the lack of a whole-of-government security strategy, lack of a horizon-scanning function and comprehensive assessment of threats, and lack of coordination and barriers to information sharing between agencies were repeated by the Cullen/Reddy review in their report, and the Royal Commission in its report. We repeat them in this report. The difficulties referred to in the Auditor-General's 2017 report resulting from outdated or incompatible legislation in the context of information sharing at the border are still apparent today, as we have noted.

A gap in oversight?

4.67. We have concluded that a gap exists in the current oversight arrangements under the ISA. It is that no independent assessment is undertaken of the effectiveness of the Agencies in fulfilling their functions under the ISA. To explain this conclusion, we recall three features of the ISA.

---

[204] Kevin Bernard Brady, CNZM *Managing Threats to Domestic Security* (Office of the Auditor-General, October 2003).
[205] Lyn Provost, CNZM *Governance of the National Security System* (Office of the Auditor-General, November 2016).
[206] Greg Schollum *Border Security: Use of Information to Process Passengers* (Office of the Auditor-General, June 2017).

4.68. First, under s 3, the ISA's purpose is to protect New Zealand as a free, open and democratic society by (among other things) establishing intelligence and security agencies that will **effectively** contribute to three sets of interests. Section 3(c)(iii) goes on to state it is a purpose of the ISA to **ensure** the Agencies' functions are performed in a manner that facilitates **effective democratic oversight**. Section 17(d) requires the Agencies to act in such a manner when performing their functions. We think it would be surprising if the concept of "effective democratic oversight" did not include assessment of how effective the Agencies were in fulfilling their legislatively mandated functions and thus meeting the overall purpose of the ISA.

4.69. Second, s 156(1) of the ISA describes the purpose of Part 6 of the ISA as being to provide for **independent** oversight of the Agencies to ensure the Agencies act with propriety and operate lawfully **and effectively**. To achieve this purpose, s 156(2) of the ISA continues both the office of Inspector-General and the Intelligence and Security Committee.

4.70. The description of the functions of the Inspector-General and the Committee, however, make no mention of assessing the effectiveness of the Agencies in contributing to the protection of national security, New Zealand's international relations and well-being and its economic well-being, apart from the Inspector-General's limited role in assessing the effectiveness of the Agencies' systems and procedures to ensure compliance with the law and operational controls.

4.71. Although the Intelligence and Security Committee functions set out in s 193 do not expressly state that the Committee is to assess the effectiveness of the Agencies, the language of the Committee's first function – "to examine the policy, administration and expenditure of each intelligence and security agency" – could possibly have been interpreted expansively to include examining effectiveness. It is clear, however, from our discussions with past and present members of the Committee that, to date, the Committee has not regarded assessing the Agencies' effectiveness as part of its role. In any event, as presently configured, it could not perform that role in a meaningful way.

4.72. Third, s 236(3)(a) permits the Prime Minister, after consultation with the Intelligence and Security Committee, to set terms of reference for a periodic review that may include "any matter relevant to the functions, effectiveness, and efficiency of [the Agencies] and their contribution to national security". The reviewers must prepare a report, which must be submitted to the Committee.[207] This provision is important for two reasons.

- It is an explicit statutory recognition that the Agencies' effectiveness in fulfilling their functions under the ISA can, and should be, independently assessed.
- The review process takes place under the general auspices of the Intelligence and Security Committee, which suggests that such issues are within its general purview despite there being no specific mention of them in the statement of the Committee's functions.

4.73. Despite what we regard as clear statutory indications that the effectiveness of the Agencies in fulfilling their essential functions should be subject to oversight under the ISA, no such assessment is presently occurring through the ISA's oversight mechanisms.

4.74. We acknowledge that the Agencies are subject to various measures that apply to other public sector agencies. The Agencies are both 'departments' for the purposes of the Public Service Act 2020. The Public Service Commissioner is the employer of the Directors-General and provides them with written performance expectations, against which they are assessed. An Assistant

[207] Intelligence and Security Act 2017, s 238.

Public Service Commissioner is also assigned to the Agencies. That person holds an appropriate security clearance and reviews a range of performance-related information and meets regularly with the Directors-General. The Public Service Commissioner will discuss the performance of the Directors-General with the responsible Minister and Prime Minister from time to time. And the Agencies were subject to Performance Improvement Framework (or PIF) reviews in 2014 and 2018.

4.75. But our purpose is to review the ISA. As noted, Part 6 states that it provides for independent oversight to ensure the Agencies operate effectively. In fact, there is no independent oversight under Part 6 to ensure the Agencies are operating effectively. We return to this issue in chapter 12.

CHAPTER 05
Protection of national security: Reflecting New Zealand's identity

Introduction

5.1. In this chapter we identify and discuss the following significant issues relating to the protection of national security in a way that reflects Aotearoa New Zealand's identity as a country:

- the meaning of 'national security'
- priority setting
- the need for the two core intelligence and security agencies (the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS), referred to as 'the Agencies'), and the intelligence and security system more generally, to reflect te Tiriti o Waitangi/the Treaty of Waitangi and the fact that New Zealand is a multi-cultural and diverse society
- section 19 of the Intelligence and Security Act 2017 (ISA).

What is 'national security'?

5.2. As noted in chapter 1, the ISA does not contain a definition of national security even though one of the three principal objectives of the Agencies is to contribute to the protection of New Zealand's national security.[208] For many years, New Zealand has adopted a broad approach to the concept of national security, applying it across a full spectrum of hazards and risks.[209] We discuss this 'all hazards, all risks' approach shortly, but note here that it is all-encompassing, covering risks from both natural disasters as well as human actors.

5.3. Along with contributing to the protection of national security, the NZSIS and GCSB have the objectives of contributing to New Zealand's international relations and well-being and to New Zealand's economic well-being. As we note in chapter 1, the statement of the Agencies' three principal objectives in s 9 of the ISA was based almost word for word on the statement of the GCSB's objective in s 7 of the Government Communications Security Bureau Act 2003, as amended in 2013. Although, under that Act, the GCSB could not undertake activities against New Zealanders; rather, its activities were to be focused on foreign intelligence.

[208] Intelligence and Security Act 2017, s 9.

[209] National Security Systems Directorate of the Department of the Prime Minister and Cabinet *National Security System Handbook* (DPMC, August 2016).

5.4. Some commentators have criticised the absence of a definition of national security in the ISA and the breadth of the Agencies' other principal statutory objectives. For example, Dr Damian Rogers has written:[210]

> The omission of a definition of national security is significant as pt 2 of the Intelligence and Security Act 2017 reframes the principal objectives of New Zealand's main intelligence Agencies in terms of three high level themes: national security; international relations and well-being; and economic well-being. Without defining any of these key terms, the language of this new Act nevertheless presents national security as something distinct from New Zealand's international relations and well-being, and from New Zealand's economic well-being. In doing so it dissolves the hitherto strong connection between intelligence-gathering activities and the pursuit of national security. This leads to the NZSIS and the GCSB being recast as *intelligence and security* agencies that exist in order to contribute not only to New Zealand's national security by providing security intelligence and protective services, but also to New Zealand's international and economic well-being through the provision of various outputs. This reframing of objectives thus radically expands the operating environment for the NZSIS and the GCSB, which is now limited only by the elasticity of these vaguely worded objectives.

5.5. The potential breadth of the Agencies' objectives and lack of a definition of national security were also raised by some we consulted with or who made submissions as deficiencies in the ISA, including Māori.

5.6. Before discussing this further, we set out the relevant background.

Background to current 'no-definition' approach

5.7. The Cullen/Reddy report had recommended that a definition of national security be included in the ISA and there was a definition in the Bill as introduced.[211] It provided:

> national security means the protection against—
>
> (a) threats, or potential threats, to New Zealand's status as a free and democratic society from unlawful acts or foreign interference: imminent threats to the life and safety of New Zealanders overseas:
>
> (b) threats, or potential threats, that may cause serious harm to the safety or quality of life of the New Zealand population:
>
> (c) unlawful acts, or acts of foreign interference, that may cause serious damage to New Zealand's economic security or international relations:
>
> (d) threats, or potential threats, to the integrity of information or infrastructure of critical importance to New Zealand:

---

[210] Damien Rogers "Intelligence and Security Act 2017: A Preliminary Critique" [2018] NZ L Rev 657 at 675. By way of additional context, the Intelligence and Security Act 2017 (ISA) replaced four pieces of legislation including the New Zealand Security Intelligence Service Act 1969 and the Government Communications Security Bureau Act 2003. Under the 1969 Act, the NZSIS had broad functions including "to obtain, correlate, and evaluate intelligence relevant to security, and to communicate any such intelligence to such persons, and in such manner, as the Director considers to be in the interests of security". The original Government Communications Security Bureau Act of 2003 was amended in 2013 to include the objective of contributing to New Zealand's national security, international relations and well-being, and economic well-being.

[211] Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM *Intelligence and Security in a free Society – Report of the First Independent Review of Intelligence and Security in New Zealand* (February 2016) at [5.83].

> (e) threats, or potential threats, that may cause serious harm to the safety of a population of another country as a result of unlawful acts by a New Zealander that are ideologically, religiously, or politically motivated:
>
> (f) threats, or potential threats, to international security.

5.8. As can be seen, the definition dealt mainly with various threats or potential threats, although it also referred to unlawful acts or foreign interference that might damage New Zealand's economic security or international relations.

5.9. Submitters on the Bill tended to support the retention of a definition. For example, the Inspector-General of Intelligence and Security argued that the Bill should contain a definition of national security because a concept so fundamental to the scheme of the Bill should not be left undefined.[212] However, the Inspector-General also noted the tension inherent in a definition: it would be a threshold for the exercise of highly intrusive powers and so must set boundaries but at the same time must recognise a broad and evolving range of threats.[213]

5.10. Officials did not support the inclusion of a definition in the Bill, however. This was against the background that they considered that the definition was important:[214]

> … for the sole reason of being determinative of when the NZSIS and the GCSB may obtain a warrant targeting a New Zealander directly and when permission to access restricted information under subpart 3 of Part 5 may be granted in respect of a New Zealander.

They thought the definition was uncertain and considered that this objective could be achieved by other means.

5.11. The select committee considering the Bill (the Foreign Affairs, Defence and Trade Committee), accepted the officials' advice and recommended the proposed definition be removed on the basis that its scope was uncertain, to the extent that it would be difficult to apply in practice, requiring the Agencies "to make difficult judgements about when the definition applied, and when their powers could be invoked".[215]

5.12. The select committee also considered that, if there was no definition in the legislation, it would be necessary to use other means to constrain the activities the Agencies could undertake to protect national security where those activities were directed at New Zealanders.[216] The committee said:

> In our view more certainty is needed, and we recommend replacing the definition of national security in clause 5 with new clause 55A. This clause would define the circumstances in which the intelligence and security agencies may take action, in respect of New Zealanders, in pursuit of their national security objective. The clause provides a closed list of things that could be broadly described as matters of national security.

5.13. Clause 55A of the Bill became s 58 of the ISA. This section provides that a warrant for the protection of national security may only be issued to permit activities directed at New Zealanders

---

[212] Inspector General of Intelligence and Security *Supplementary Submission on the Intelligence and Security Bill* (9 November 2016) at 4.

[213] Other parties arguing for the inclusion of a definition included the Legislation Design and Advisory External Subcommittee and the New Zealand Law Society.

[214] Department of the Prime Minister and Cabinet *New Zealand Intelligence and Security Bill: Departmental Report to the Foreign Affairs, Defence and Trade Committee* (December 2016) at [120].

[215] Foreign Affairs, Defence and Trade Committee *New Zealand Intelligence and Security Bill* (24 February 2017) at 3.

[216] By 'New Zealanders' in this context we mean New Zealand citizens and permanent residents.

if it is necessary to contribute to the protection of national security **and** relates to any of various harms specified in s 58(2).[217] Among the specified harms are terrorism, violent extremism, certain forms of espionage or other foreign intelligence activity, sabotage, proliferation of weapons of mass destruction, certain forms of serious crime (mainly transnational in nature),[218] and threats to or interference with information (including communications) or information infrastructure of importance to the New Zealand government. The harms also include threats against New Zealand's sovereignty or government operations and, provided they have the potential to adversely affect New Zealand's interests, threats against international security.[219] Such a warrant may only be issued by the Minister and a Commissioner for Intelligence Warrants acting together.

5.14. Some of the specified harms in s 58 incorporate broadly worded concepts, for example: foreign intelligence activity directed at "a New Zealand interest (whether or not that interest is in New Zealand)";[220] "anything that may be relevant to serious crime" (defined to mean any offence punishable by three or more years' imprisonment) that "originates outside New Zealand or is influenced from outside New Zealand";[221] and "threats to international security that have the potential to impact adversely on New Zealand's interests".[222]

5.15. Despite that, the harms mentioned largely fall within a conventional conception of national security. Accordingly, to the extent it applies at all to the ISA, the expansive 'all hazards, all risks' approach to national security does not operate in relation to New Zealanders.[223] That said, national security is not limited in this way where the relevant Minister is asked to issue a warrant directed at non-New Zealanders for the protection of national security. There, the Minister simply has to be satisfied that the activity sought to be authorised is necessary to contribute to the protection of national security (the criteria in s 61 must be met as well), so it is possible a broader approach could be taken.

5.16. A similar regime applies to access to 'restricted information' (for example, confidential information held by the Inland Revenue Department). To obtain access to such information about a New Zealander in order to protect national security, the Director-General of an Agency must apply to the relevant Minister and the Chief Commissioner of Intelligence Warrants for permission.[224] The Minister and a Commissioner may give permission if they are satisfied that access to the restricted information is necessary to contribute to the protection of national security **and** to help in protecting against any of the harms specified in s 58(2).[225] However, in relation to restricted information about a non-New Zealander, the relevant Minister, acting alone, may give permission if satisfied simply that access is necessary to contribute to the protection of national security.[226]

---

[217] The criteria in s 61 must also be met, but they can be put to one side for present purposes.

[218] 'Serious crime' is defined for these purposes as an offence punishable by more than three years' imprisonment: see Intelligence and Security Act 2017, s 47.

[219] A different section, s 59, provides for the issue of warrants against New Zealand citizens or permanent residents to contribute to New Zealand's international relations or economic well-being in limited circumstances.

[220] Intelligence and Security Act 2017, s 58(2)(b).

[221] Section 58(2)(e).

[222] Section 58(2)(g)(i).

[223] It is possible, for example, that a pandemic might lead to social disruption on such a scale that it threatened the operations of the government, which is a harm identified in s 58(2)(g).

[224] Intelligence and Security Act 2017, ss 136(1) and (2)(a).

[225] Section 137(a). The criteria set out in s 139 must also be met.

[226] Intelligence and Security act 2017, ss 136(2)(b) and 138. Again, the criteria in s 139 must be met.

5.17. Two points emerge from this.

- It might be argued that the absence of a definition of national security is not significant in respect of New Zealanders because of the additional requirement that an authorisation must also relate to one of the harms specified in section 58(2).
- The fact, however, that it has been possible to list these harms for the purposes of a protection of national security intelligence warrant in respect of a New Zealander means it must also be possible to define national security for ISA purposes by reference to these harms without creating excessive uncertainty.

Our assessment

5.18. As noted, New Zealand has applied the all hazards, all risks approach to national security for many years and the Cabinet confirmed it in 2001 (although, as noted below, Cabinet has recently decided in principle to adopt a more focused approach). The thinking behind it was that threats to New Zealand and its people come not only from traditional security concerns – sabotage, terrorism, transnational organised crime – but also from hazards like pandemics, which have the potential to affect many New Zealanders; biosecurity threats, which may undermine the country's productive capacity; and large-scale natural disasters. This broad approach has an obvious attraction in the context of emergency preparedness, where the source of the threat is less important than its consequences, and it accommodated the fact that the threatscape changes over time as new threats emerge.

5.19. In its 2016 Handbook on the National Security System, the Department of the Prime Minister and Cabinet noted that seven main objectives underpin the all hazards, all risks approach:[227]

- **ensuring public safety** – providing for, and mitigating risks to, the safety of citizens and communities (all hazards and threats, whether natural or man-made)
- **preserving sovereignty and territorial integrity** – protecting the physical security of citizens, and exercising control over territory consistent with national sovereignty
- **protecting lines of communication** – these are both physical and virtual and allow New Zealand to communicate, trade and engage globally
- **strengthening international order to promote security** – contributing to the development of a rules-based international system, and engaging in targeted interventions offshore to protect New Zealand's interests
- **sustaining economic prosperity** – maintaining and advancing the economic well-being of individuals, families, businesses and communities
- **maintaining democratic institutions and national values** – preventing activities aimed at undermining or overturning government institutions, principles and values that underpin New Zealand society
- **protecting the natural environment** – contributing to the preservation and stewardship of New Zealand's natural and physical environment.

[227] National Security Systems Directorate of the Department of the Prime Minister and Cabinet *National Security System Handbook* (DPMC, August 2016) at 8.

5.20. Obviously, these objectives are broad, and some are beyond the practical capacity of the Agencies to address. For example, from the Agencies' perspective, there is a major difference between disruption caused by sabotage or a cyber-attack, which result from human actions, and disruption caused by a natural disaster such as a major earthquake. Whereas it is part of the Agencies' role to seek to prevent sabotage or cyber-attacks from occurring, they can do nothing to prevent earthquakes. Their interest in natural disasters is principally in the aftermath: are malicious actors attempting to take advantage of the situation in some way that creates significant risks for New Zealand, its institutions or people? This raises a question as to the utility of a broad approach to "national security" in the context of the Agencies.

5.21. In July 2022, as part of a review of New Zealand's national security policy settings, the Cabinet External Relations and Security Committee agreed in principle to adopt a more focused concept of national security in place of the all hazards, all risks approach.[228] The new concept was based on "actively protecting New Zealand from malicious threats to national security interests from those who would do the country harm", with this approach forming part of the development of a national security strategy.[229] It was felt this approach would be more capable of implementation and avoid the unnecessary 'securitisation' of issues and communities. It would also be accompanied by an approach that would build connections with other sectors, to monitor and address the national security implications that flow from other areas, such as climate change. The national security interests referred to at the time were identified as protecting:

- New Zealanders at home and abroad
- New Zealand's sovereignty and territorial integrity
- democratic institutions and norms, including universal human rights and te Tiriti o Waitangi/the Treaty of Waitangi
- national economic security
- the wider maritime region and connections to the world, both physical and digital
- a peaceful, stable, prosperous and resilient Pacific underpinned by strong regionalism and in which New Zealand has the freedom to act in support of shared interests and values
- a strong international rules-based system in the Indo-Pacific and beyond, centred on multilateralism, liberal democratic values and the promotion of peace
- a strong network of partnerships within and beyond New Zealand.

5.22. This approach was approved in principle by Cabinet on 19 July 2022, subject to a public engagement process (which has since led to some changes).[230]

5.23. International good practice suggests the ISA should contain a definition of what is a fundamental mandate of the Agencies, namely, to contribute to the 'protection of national security'. At the request of the United Nations Human Rights Council, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism prepared a report containing a compendium of good practices that emerged from a detailed consultation

[228] Cabinet External Relations and Security Committee, Minute of Decision, ERS-22-Min-0028 (19 July 2022). Note that the wording of the concept has since changed to say, "actively protecting New Zealand from threats that would do us harm".

[229] Above n.

[230] A summary of the public consultation process can be read on the website of the Department of the Prime Minister and Cabinet *Kōrero on the development of Aotearoa New Zealand's first national security strategy* (online, 12 December 2022) <dpmc.govt.nz/our-programmes/national-security/aotearoas-national-security-strategy>.

process examining the practices of numerous states in relation to their intelligence and security agencies.[231]

5.24. The first set of good practices deals with an agency's mandate and legal basis. Practice 2 is described as follows:[232]

> The mandates of intelligence services are narrowly and precisely defined in a publicly available law. Mandates are strictly limited to protecting legitimate national security interests as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address. If terrorism is included in these threats, it is defined in narrow and precise terms.

5.25. Despite this statement of good practice, and the common use of the concept of national security in contexts besides the work of intelligence and security agencies (such as overseas investment decisions), many states do not define national security, or define it only in some contexts or in general terms. A concern about a definition is that it is feared it might constrain the ability of intelligence and security agencies to respond to new threats as they arise. Besides that, it is a difficult concept to capture in a definition.

5.26. While the 'protection of national security' mandate of the Agencies is limited in respect of New Zealanders by s 58 of the ISA, it is not limited in other contexts. Despite the difficulties of developing a suitable definition, we think it undesirable in principle that a term that is fundamental to the structure and operation of the ISA be left undefined, with any limits on its scope being imposed only in particular contexts. This is consistent with the view of the United Nations Human Rights Committee, which in the context of discussing the right to privacy under the International Covenant on Civil and Political Rights, expressed concern over the absence of a clear definition of the term 'national security' in New Zealand legislation.[233] It follows that we do not agree with officials' advice to the select committee that the definition recommended in the Cullen/Reddy report was important solely because it identified the circumstances in which intelligence and security warrants could be obtained against New Zealanders. The term 'national security' has a more extensive role in the ISA than that.

5.27. The following references illustrate the wider importance of national security in the legislation.

- The purpose of the ISA is to protect New Zealand as a free, open and democratic society, by (among other things) establishing intelligence and security agencies that will effectively contribute to the protection of New Zealand's national security: s 3(a)(i).
- One of the principal objectives of the Agencies is to contribute to the protection of New Zealand's national security: s 9(a).
- Sections 58 and 60 provide for the issue of warrants to authorise otherwise unlawful activities that are necessary to contribute to the protection of national security.

---

[231] *Report of the Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism, Martin Scheinin: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence Agencies while countering terrorism, including on their oversight* A/HRC/14/46 (17 May 2010).

[232] Above n, at [10].

[233] See United Nations Human Rights Committee, *Concluding Observations on the Sixth Periodic Report of New Zealand* UN Doc CCPR/C/NZL/CO/6 (28 April 2016) at [15]. The Act mentioned was the Telecommunications (Interception Capability and Security) Act 2013, but we consider that the same comment applies more broadly.

- Periodic reviews, such as the present, may be required to consider "any matter relevant to the functions, effectiveness and efficiency of [the Agencies] and their contribution to national security": s 236(2)(a).

So, contributing to the protection of national security is one element of the essential purpose of the ISA and, reflecting that, is one of the principal objectives of the Agencies. The Agencies may be authorised to undertake unlawful activities necessary to contribute to that objective. Yet the concept is undefined, even though, potentially, it bears wide and narrow meanings.

5.28. We appreciate that, from a practical perspective, access to resources is likely to place an effective limit on the scope of the Agencies' activities. Limited resources mean the Agencies are likely to focus on what would be generally accepted as their core responsibilities, although that is not inevitable given the efforts the Agencies make to respond to customer requirements. But we do not see that as a reason for not having a definition of national security in the ISA.

5.29. As we see it, good legislative design requires that a term that plays a fundamental role in legislation as national security or, alternatively, protection of national security does in the ISA should have, or be given, as clear a meaning as reasonably possible. This is especially so where the term can be interpreted either narrowly or more widely, as is the case with national security.[234] A definition would provide important context within which the Agencies and those with oversight responsibilities would be expected to act, for example, the Agencies when seeking warrants, the Minister and the Commissioners of Intelligence Warrants when considering whether to grant them and the Inspector-General when reviewing their issue and application. It would also help the Intelligence and Security Committee in performing its functions.

5.30. In addition, an important function of legislation such as the ISA is to inform the public of the role of the Agencies. This should be done in as direct and straightforward a way as practicable. A clear statement of what is being protected at the outset of the ISA would facilitate this. Submitters to the review also raised this point, with some noting that the absence of a definition means the ISA could potentially be applied to a broad range of people and situations, resulting in unnecessary invasions of privacy.

5.31. What then should the definition be? Broadly, there are two options. The first is to adopt a definition that attempts to identify the threats the Agencies should protect against. The Canadian Security Intelligence Service Act provides an example:[235]

> *threats to the security of Canada* means
>
> (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
>
> (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
>
> (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and

[234] We note that the Immigration Act 2009 contains several provisions intended to protect New Zealand from people who are security threats. Section 4 of the Act contains a definition of 'security'.

[235] Canadian Security Intelligence Service Act RSC 1985 c C-23, s 2.

> (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,
>
> but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

A similar definition is provided in the Australian legislation.[236] We note the list of harms in s 58(2) of the ISA, which applies where 'protection of national security' warrants are sought in respect of New Zealanders is, in combination with s 58(1)(a)(ii), effectively a definition of this type, although it serves a different purpose in the ISA.

5.32. While this form of definition has the advantage of providing a degree of specificity, which would help the Agencies, oversight officials and the public, the risk is it may not be sufficiently flexible to protect against threats that will emerge in the future. This is an area where adaptability to a changing threat environment is particularly important.

5.33. The second option is to frame the definition at a more general level, in terms of threats to the essential elements of New Zealand as a 'free, open and democratic society', that is, to the fundamental features of New Zealand's democracy, its way of life and the safety of its communities and people. The threats should be ones that Agencies could counteract, which would exclude threats from natural disasters unless those national disasters became the setting for human activity directed at, for example, undermining New Zealand's democratic institutions. We give two examples of the type of definition we have in mind.

5.34. The first example comes from Europe. In 2019, the Council of Bars and Law Societies of Europe (CCBE) published a report containing recommendations on the protection of fundamental rights in the context of national security.[237] As part of their work, the CCBE conducted a survey of how national security operated as a legal concept in 11 of their member states.

5.35. The CCBE's report drew an important distinction between, on the one hand, the nature of national security, which remains relatively constant, and, on the other, the manner in which national security is threatened, which is constantly changing. The nature of national security includes the fundamental characteristics of the state that require protection. The report suggested a definition that sought to identify what the concept of national security covered in the following terms:[238]

> National security is understood as the internal and external security of the State, which consists of one or more of the following elements:
>
> - the sovereignty of the State;
> - the integrity of its territory, its institutions and its critical infrastructure;
> - the protection of the democratic order of the State;
> - the protection of its citizens and residents against serious threats to their lives, health and human rights;
> - the conduct and promotion of its foreign relations and commitment to the peaceful coexistence of nations.

---

[236] See definition of 'security' in the Australian Security Intelligence Organisation Act 1979 (Cth), s 4.

[237] Council of Bars and Law Societies of Europe *CCBE Recommendations on the Protection of Fundamental Rights in the Context of 'National Security' 2019* (online, 2019).

[238] Above n, at 17.

5.36. The second example comes from Canada. In a recent discussion of national security strategy in Canada, Aaron Shull and Wesley Wark described national security in the following way: [239]

> National security aims to protect Canada and its people from major threats that would undermine our democratic institutions and processes, our economy, our social fabric and values, and our interests.

5.37. They went on to note that while national security is a "portmanteau phrase", this definition uses concepts that reflect contemporary reality: protection, major threats, democracy, economy, societal cohesion and interests. The definition refers both to the state and its people and does not distinguish between threats from internal or external (ie, foreign) sources. An important feature of the definition is the nature of the threat: it must be 'major' and, if it transpired, 'would' undermine one or more of the matters listed.

5.38. We see value in incorporating this form of definition in the ISA, although we would define 'protection of national security' rather than 'national security' standing alone because this is generally the context in which national security appears in the ISA. The Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019 (the Royal Commission) emphasised that it is necessary to promote greater public engagement with national security issues and the roles of the Agencies in protecting New Zealand's national security.[240] Public understanding is a prerequisite to meaningful public engagement. We consider that a modified version of this definition would provide greater clarity in identifying why the Agencies undertake their work. Identifying what it is that the Agencies are trying to protect illuminates what they need to do and what powers they should have. As we see it, our proposed definition is broadly consistent with the Cabinet's recent decisions in relation to national security.

5.39. A definition of 'protection of national security' along the following lines could be included in s 4 of the ISA:

> **protection of national security** means the protection of New Zealand, its communities and people from activities that are threats because they undermine, or seek to undermine, one or more of New Zealand's—
>
> (a) territorial integrity and safety, including the safety of its communities and people;
>
> (b) sovereignty, democratic institutions, processes and values;
>
> (c) multi-cultural and diverse social fabric; and
>
> (d) essential interests, including its critical infrastructure and governmental operations;
>
> and includes identifying and enabling the assessment of such threats.

5.40. The important elements of this definition are that:

- it focuses on **protection** of the **nation**, its **communities** and **people**
- from **threats**[241]

---

[239] Aaron Shull and Wesley Wark *Reimagining a Canadian National Security Strategy* (Centre for International Governance Innovations, Special Report, 6 December 2021) at 9.

[240] Royal Commission of Inquiry *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) at part 10, chapter 2.2 (Royal Commission report).

[241] The description of "national security" given at paragraph [5.36] refers to "major threats". We considered whether our proposed definition at [paragraph [5.39] should refer to "significant threats" rather than simply "threats". We decided that

- the threats must be in the form of **activities**, which indicates they must be human-sourced, although whether the source is local or foreign-based is irrelevant
- the activities must have a **specified effect or purpose**
- the specified effect or purpose must go to **undermining** any of the matters listed
- the matters listed go to New Zealand's **core features as a democratic state**, its **characteristics as a country**, its **safety** and **essential interests** (which could include economic interests).

5.41. We consider that this definition would capture the threat-based work currently undertaken by the Agencies: investigation of possible sabotage, espionage, terrorism, extremism, transnational crime, foreign interference, cyber threats and so on wherever they are generated. It would cover matters such as the spread of state-sponsored disinformation in the context of, say, a global health crisis such as the COVID-19 pandemic, which might undermine safety and social cohesion. It would also cover threat discovery work. The definition does not attempt to list specific threats of the type just mentioned, although such threats could be listed as non-exhaustive examples as suggested during our consultations. That may be useful, but it would have to be done in a way that ensured the definition was capable of covering new and emerging threats in a world that is, from political, technological and other perspectives, highly dynamic. For example, a sentence along the following lines could be added at the end of the definition:[242]

> Such activities include, but are not limited to, terrorism, espionage, sabotage, violent extremism, insurrection, foreign interference, cyber threats, and serious transnational crime.

Other examples (such as money laundering) could be added if that was thought appropriate.

5.42. The definition may be criticised as being too general to constrain or guide the Agencies and those who oversee their activities. We accept there is some force in that criticism. We note, however, that the same criticism applies to the list of harms in s 58, as noted at paragraph [5.14], and to other attempted definitions. That the application of the definition requires some exercise of judgement does not necessarily destroy or diminish its value. Rather, the definition's value must be assessed against the fact that it would operate within the context of the ISA as a whole. If the mechanisms established by the ISA to constrain the Agencies operate effectively – the government's priority-setting responsibilities, the authorisation duties of the Minister and the Commissioners of Intelligence Warrants, the Inspector-General's review function and so on – the definition would serve a useful function. It would focus attention on the fundamental features of New Zealand that the Agencies are intended to play a part in protecting and, through that, would help identify what it is they should be protecting us from.

5.43. In short, we consider the proposed definition would serve an important purpose in identifying what it is that needs protection. It would provide the Agencies and those responsible for their control and oversight a sufficient basis to guide and assess their actions.

5.44. While this definition of protection of national security would capture a range of internally-generated and foreign-generated threats, it would not capture all the work the Agencies legitimately undertake. While they identify threats of various types, the Agencies also contribute

---

adding the qualification "significant" might create uncertainty in relation to the scope of the Agencies' threat discovery work, and so decided to omit it. However, the issue is debatable and could be given further consideration.

[242] We note that this approach is used elsewhere in the Intelligence and Security Act 2017: s 202(2) gives examples of the kinds of information that fall within the definition of 'sensitive information' in s 202(1).

to New Zealand's essential interests (including essential economic and international interests) in other ways. For example, an agency may gather data in relation to geopolitical developments that, while not constituting an immediate threat to New Zealand, have the potential to affect the country in the future. Similarly, events in a particular overseas jurisdiction may be of interest to New Zealand even though they pose no particular threat to the country for the foreseeable future.

5.45. Accordingly, in addition to contributing to the protection of national security (as defined), the Agencies should be empowered to contribute to New Zealand's essential interests in the absence of activities that constitute a threat to New Zealand, its communities or its people. If the definition we have proposed (or something like it) were to be adopted, s 3(a) and s 9 could remain as presently drafted, although activities constituting a threat should be dealt with on a 'protection of national security' basis rather than a 'contributing to international relations' basis. This is because it is important in the context of both oversight and public understanding to identify what proportion of the Agencies' work responds to perceived threats and what is more general in nature. We consider this may need to be made explicit in the ISA and suggest a reporting obligation that we address further in chapter 7.

RECOMMENDATION 02

Amend section 4 (Interpretation) of the Intelligence and Security Act 2017 to include a definition of "protection of national security" along the following lines:

> **"protection of national security"** means the protection of New Zealand, its communities and people from activities that are threats because they undermine, or seek to undermine, one or more of New Zealand's—
>
> (a) territorial integrity and safety, including the safety of its communities and people;
>
> (b) sovereignty, democratic institutions, processes and values;
>
> (c) multi-cultural and diverse social fabric; and
>
> (d) essential interests, including its critical infrastructure and governmental operations;
>
> and includes identifying and enabling the assessment of such threats.

with the possible addition of wording such as:

> Such activities include, but are not limited to, terrorism, espionage, sabotage, violent extremism, insurrection, foreign interference, cyber threats and serious transnational crime.

Priority setting

5.46. As described, when the select committee recommended that no definition of national security be included in the ISA, it recommended a measure designed to limit the scope of the activities of the Agencies in relation to New Zealanders, namely, the insertion of s 58. Another potentially significant limitation is found in s 10(1)(a), which provides that it is a function of the intelligence and security Agencies to "collect and analyse intelligence **in accordance with the New Zealand Government's priorities**" (emphasis added). In the absence of a definition of national security, a

specifically stated set of priorities may well have the effect of significantly narrowing the potential scope of the Agencies' activities.

5.47. Consideration of national security priority setting was an important part of the Royal Commission's work. The Royal Commission's terms of reference required it to make findings about "whether relevant [public] sector agencies failed to anticipate or plan for the terrorist attack due to an inappropriate concentration of counter-terrorism resources or priorities on other terrorism threats … which was not based on an informed assessment of the threats of terrorism associated with other ideologies". While this was relatively specific in nature, the Royal Commission undertook a more general consideration of the process of priority setting for the National Assessments Bureau and the Agencies, which provides helpful background.[243]

5.48. In its report, the Royal Commission noted that, generally, the Agencies have treated the government's priorities referred to in s 10(1)(a) as those set out in the Government's National Security Intelligence Priorities (now commonly referred to as the NSIPs).[244] The Royal Commission considered that the NSIPs were too general to provide effective guidance to the Agencies and did not enable appropriate decision-making on a system-wide basis, noting that the NZSIS had developed its own 10-year operational strategy.[245] The Royal Commission considered that greater coordination across the whole security and intelligence sector was required.[246]

5.49. The Royal Commission also raised another important point. As their annual reports show, the Agencies, particularly the GCSB, have a strong customer focus and attempt to respond to the requirements of their customers. While this focus is understandable (especially in a cyber-security context), it does have the risk that customer requirements set the agenda, and these may not necessarily coincide with the most pressing national security needs of the country. As the Royal Commission noted when discussing the National Assessments Bureau:[247]

> … the National Assessments Bureau primarily addressed topics or themes on which its customers – usually the Ministry of Foreign Affairs and Trade – had asked for assessments. This explains its focus on foreign policy, security and trade issues, as highlighted by the 2014 Performance Improvement Framework review of the New Zealand Intelligence Community. That review observed that the National Assessments Bureau's customers were reluctant to accept a reduction in foreign policy assessments in favour of a greater attention to national security issues.

5.50. The Royal Commission concluded that "the threat of domestic terrorism was not a priority for the National Assessments Bureau and it did not provide any assessments solely focused on domestic terrorism". This created the assessment gap that the Royal Commission found had contributed to "an inappropriate concentration of resources on the threat of Islamic terrorism" in the NZSIS.[248]

5.51. The Royal Commission also observed that, generally, leadership and coordination "was limited with the relevant public sector agencies operating largely independently and in parallel" and noted the importance of the connection between priorities and resourcing.[249] This finding is also

[243] Royal Commission report, at part 8, chapter 3.
[244] Royal Commission report, at part 8, chapter 14, [8].
[245] Royal Commission report, at part 8, chapter 3, [66].
[246] Royal Commission report, at part 10, chapter 2.2.
[247] Royal Commission report, at part 8, chapter 4, [22].
[248] Royal Commission report, at part 8, chapter 4, [19].
[249] Royal Commission report, at part 8, chapter 1, [8].

consistent with independent reviews of the intelligence community dating back to the Auditor-General's first performance audit report in 2003.[250]

5.52. The NSIPs are prepared by the National Intelligence and Risk Coordination Directorate (working with the National Intelligence Coordination Committee). This is a unit of the Department of the Prime Minister and Cabinet, in fulfilment of the chief executive's responsibility for advising Ministers on the setting of priorities for intelligence collection and analysis.[251] The priorities are reviewed periodically by Cabinet, generally every three years, and a public version is available.[252] The most recent priorities set in December 2021 are due to be reviewed by December 2023.[253]

5.53. The 2021 NSIPs contain 13 priorities, identified by the following headings:

- biosecurity and human health
- climate change and environmental issues
- emerging, critical and sensitive technology
- foreign interference and espionage
- global economic security
- foreign interference and sabotage
- global governance and strategic competition
- malicious cyber activity
- maritime, border security and Antarctica
- New Zealand's strategic interests in the Asia region
- New Zealand's strategic interests in the Pacific region
- terrorism and violent extremism
- threats to New Zealanders overseas
- transnational and organised crime.

5.54. For each priority, a general description is provided of what it entails.[254]

5.55. The NSIPs were approved by Cabinet on the recommendation of the Minister for National Security and Intelligence. The Minister's paper to Cabinet described the role of the NSIPs as follows:[255]

> The NSIPs are a guide to all agencies that may be able to provide intelligence. Agencies' resources are not unlimited, and tough prioritisations decisions need to be made. Ultimately, decisions about where they focus effort are up to individual agencies, but they need to be making these decisions within the parameters set out in the NSIPs, and with consideration about the collective allocation of effort. Therefore, in line with previous iterations, the NSIPs are scoped broadly, giving agencies discretion within the

[250] Kevin Bernard Brady, CNZM *Managing Threats to Domestic Security* (October 2003) at [3.19].
[251] Intelligence and Security Act 2017, s 233(1)(b).
[252] DPMC "National Security Intelligence Priorities" (2021) <dpmc.govt.nz/our-programmes/national-security/national-security-intelligence-priorities>.
[253] Cabinet paper "National Security Intelligence Priorities: 2021 Review Minute of Decision" (8 December 2021) at [14.2].
[254] Above n 252.
[255] Cabinet Paper "2021 updated National Security Intelligence Priorities" (16 November 2021).

> 13 priority areas to provide intelligence on issues that align with their unique capabilities and resources.

5.56. In response to the Royal Commission's recommendation that the Agencies be provided with more detail to help them make informed decisions about where to allocate resources, the National Intelligence Coordination Committee developed a new 'key areas of focus' section to help with decision-making.[256] The Cabinet paper said:[257]

> *Key areas of focus* are a new addition to the NSIPs and one I believe will provide increased assurance that our intelligence agencies are focusing effort in the most important areas. Under the previous framework, potentially any public sector agency is accountable for the delivery of the NSIPs, which presents issues in clearly identifying expectations, and roles and responsibilities. Under the proposed framework, there is now an identifiable collection of agencies responsible for reporting against the NSIPs.

5.57. The key areas of focus are based on classified intelligence requirements, which are developed with customers and intelligence agencies.

5.58. Of course, the specialised capabilities of the GCSB, NZSIS and National Assessments Bureau will sometimes be used for activities outside the NSIPs. Examples are as follows.

- Their capabilities may be used to respond to unanticipated threats, such as the COVID-19 pandemic. Where those threats are not covered in the NSIPs or otherwise in the ISA, written ministerial approval will be given to make them priorities.
- Horizon-scanning is not explicitly addressed in the priorities. The substantial horizon-scanning exercise that the National Assessments Bureau undertakes periodically may not fit with any of the NSIPs but, despite that, is a clear priority of the government.
- Advice and assistance that the Agencies provide to the New Zealand Defence Force and New Zealand Police under s 13(1)(b) of the ISA to facilitate those authorities' performance of their "functions, duties or powers" may not involve any of the NSIPs.

5.59. Some of these activities that take place outside the NSIPs are not subject to the same degree of ministerial consideration and coordination by the Department of the Prime Minister and Cabinet as activities within the NSIPs' scope.

5.60. It is worth noting that New Zealand is not alone in wrestling with the challenge of intelligence requirements, nor is this challenge a new one. Sir Mansfield Cumming, the founder of the United Kingdom's Secret Service once remarked:[258]

> A fundamental truth about intelligence organisations: they tend to be as good or as bad, as the requirements placed upon them. If the requirements are precise, clear and important, the response … tends to be better, and failure certainly more apparent, than if the requirements are woolly, general, and not obviously relevant, producing answers as unsatisfactory as the questions.

5.61. We make three comments about the setting of the NSIPs.

---

[256] It is important emphasis that the National Intelligence Coordination Committee does not make decisions about the implementation of the NSIPs when developing the 'key areas of focus'. Decisions regarding resource allocation are left to agencies. Cabinet Paper "2021 updated National Security Intelligence Priorities" (16 November 2021) at [31]–[34].

[257] Cabinet Paper "2021 updated National Security Intelligence Priorities" (16 November 2021) at 34.

[258] Alan Judd, *The Quest for C: Mansfield Cumming and the Founding of the Secret Service* (London: HarperCollins Publishers, 2000) at 385.

- First, obviously the NSIPs are narrower than the all hazards, all risks approach to national security in that they do not include events (such as natural disasters) that would fall within an all hazards, all risks approach. To that extent, they are helpful in narrowing the potential scope of the Agencies' activities under s 10(1)(a).
- Second, the NSIPs can guide prioritisation and resourcing decisions for relevant government agencies, not just the GCSB or NZSIS and, consequently, provide only limited assistance in understanding what the Agencies do. This is because the scope of the NSIPs is broad, they are stated at a high level of generality, at least in the unclassified version, and some (given the way they are expressed) are not an obvious fit with the work of the Agencies, for example, the biosecurity and human health and climate change and environmental issues priorities.[259] The government's identification of key areas of focus may offer improvement in this context. It is useful, however, to recall an observation made by the 9/11 Commission in its report on the terrorist attacks of 11 September 2001. It said that the US intelligence community, confronted by "an overwhelming number of priorities, flat budgets, an outmoded structure, and bureaucratic rivalries", had failed to pin down the big-picture threat posed by "transnational terrorism" throughout the 1990s and up to 11 September 2001.[260]
- Third, given the broad purpose of the NSIPs and the generality with which they are stated, further steps need to be completed before the Agencies can identify their priorities in terms of s 10(1)(a) of the ISA. If the Royal Commission's call for greater transparency, greater public understanding and more public discussion of national security issues is to be answered, two steps in relation to the Agencies' priorities are required.
  - First, a full description of the way the s 10 priorities are developed needs to be prepared and made publicly available, although the description will need to recognise that unanticipated priorities may sometimes arise. In terms of the structure of the ISA, the s 10 priorities should operate as one of the controls on the work of the Agencies. Like other controls, they need to be as transparent as possible. That transparency starts with a full description of the process by which they are established. If the reality is that the Agencies' priorities are not provided to them but are essentially self-selected, that should be made clear.
  - Second, the necessary transparency should extend to identifying publicly what the Agencies' priorities actually are, stated with as much specificity as legitimate national security considerations permit. This is necessary if people are to have a realistic understanding of what it is that the Agencies actually do, which should enable meaningful public engagement and enhance the Agencies' social licence.

[259] There may, of course, be circumstances in which issues relating to biosecurity or climate change could be relevant to the work of the Agencies (eg, malicious actors attempting to take advantage of a biosecurity emergency), but they do not have the obvious relevance of matters such as counterterrorism, violent extremism, foreign interference, transnational serious and organised crime and so on.

[260] Thomas H Kean, *The 9/11 Commission Report – Final Report of the National Commission on Terrorist Attacks Upon the United States* (August 2004).

RECOMMENDATION 03

Make publicly available a full description of the process by which the Government's priorities for the collection and analysis of intelligence by the Government Communications Security Bureau and the New Zealand Security Intelligence Service (the Agencies) under section 10 of the Intelligence and Security Act 2017 are developed.

Require the publication of the Agencies' intelligence and security priorities, with as much specificity as legitimate national security considerations permit.

Reflecting te Tiriti o Waitangi/the Treaty of Waitangi and New Zealand's multi-cultural and diverse society

5.62. Given the importance of te Tiriti o Waitangi/the Treaty of Waitangi (te Tiriti) we discuss this first before discussing the significance of New Zealand being a multi-cultural and diverse society.

Te Tiriti o Waitangi/the Treaty of Waitangi

5.63. Unusually for an important modern Act of obvious relevance to Māori, the ISA makes no mention of te Tiriti or its 'principles'. Nor, indeed, did the Cullen/Reddy report. The reason may be that national security was thought to come within Article 1 of te Tiriti, as being the sole responsibility of the Crown.

5.64. Whatever the explanation, we consider that the ISA should recognise the Agencies' obligations, as public sector agencies, to have regard to te Tiriti.[261] Accordingly, we recommend that s 3(c) and s 17 of the ISA be amended to require this.

5.65. There are three reasons for this recommendation.

- First, given the rapidly developing understanding of the place of te Tiriti in New Zealand's legal framework, we think it important as a matter of principle that the ISA explicitly recognises its relevance to the work of the Agencies. This is necessary to place the work of the Agencies in its proper context in modern-day New Zealand.
- Second, the Agencies will interact with Māori in different contexts: as employees, as interested parties, as members of the public and, perhaps, as affected communities or the subjects of inquiry. Those interactions should occur within a framework that explicitly recognises the relevance of te Tiriti.
- Third, certain forms of technological development may have particular significance for Māori. For example, as the Privacy Commissioner has noted, facial recognition technology may capture images of traditional tattoos directly linked to a person's whakapapa. If an Agency wished to use such technology, issues under te Tiriti may well arise.[262]

[261] See s 14 of the Public Service Act 2020.

[262] *Office of the Privacy Commissioner position on the regulation of biometrics* (Position paper, October 2021) at 1.1, 2.1 and 3.1.

5.66. The inclusion of an explicit te Tiriti reference in the ISA received strong support through the consultation process, including from the Iwi Chairs Forum, Kāpuia, Te Hunga Rōia Māori o Aotearoa and the Human Rights Commission.

5.67. The Iwi Chairs Forum representatives argued that Māori have an obligation for public safety in the exercise of tino rangatiratanga under Article 2 of te Tiriti. To them this means questions of intelligence and security are not solely the responsibility of the Crown. Māori also have responsibilities.

5.68. In addition, the Iwi Chairs Forum representatives told us that there are several practical reasons why a specific reference to te Tiriti is appropriate. Māori feel that the Agencies lack understanding about Māori communities and perspectives. Māori communities also feel especially vulnerable to the exercise by the Agencies of their powers. Given the amount of information the Agencies gather, there are also concerns about data sovereignty.

5.69. The feedback from the Iwi Chairs Forum reflects some of our thinking on why the ISA should include an explicit reference to te Tiriti. This feedback was mirrored to varying degrees by other submitters mentioned above but not quoted.

5.70. In fact, the ideal for the Iwi Chairs Forum would be specific Māori representation at all levels of the intelligence and security community. We do not go so far as to recommend this. We consider this takes us into the level of operational decision-making within the Agencies, which is beyond our remit. Ultimately, including a reference to te Tiriti obligations in s 3(c) and s 17 ensures there is a statutory directive to the Agencies, alongside their existing obligations as public sector agencies, to ensure that te Tiriti plays a part in their decision-making. However, it gives the Agencies flexibility in determining how that directive might be given effect. This does not preclude the possibility of greater Māori representation in specific areas, but it leaves that for the Agencies to work through, desirably in discussion with Māori.[263]

New Zealand's multi-cultural and diverse society

5.71. Noting that New Zealand society is becoming increasingly diverse, the Royal Commission concluded that much greater public engagement with national security issues was necessary. In that context, the Royal Commission said the public sector had to value: (i) communities' input into decisions; (ii) transparency; and (iii) engaging in robust debate. In addition, the government needed to take the lead on two fronts:[264]

- first, to ensure New Zealand's counterterrorism effort (and, by extension, its national security effort) is valued by the people it seeks to protect
- second, to understand what New Zealand's changing demographics mean for New Zealand as a society and to promote consistent messages about the benefits of diversity and an inclusive society.

5.72. Clearly, New Zealand is becoming increasingly multi-cultural and diverse. The 2018 Census identifies six major ethnic groups in New Zealand: European (70.2%); Māori (16.5%); Pasifika (8.1%); Asian (15.1%); Middle Eastern/Latin American/African (1.5%); and other ethnicity

[263] One area specifically identified by the Iwi Chairs Forum representatives was the advisory panel to the Inspector-General, which we have recommended has an increased membership and could, potentially, include Māori or wider community representation.

[264] Royal Commission report, summary of recommendations at [8].

(1.2%).[265] But within those major groups are many other communities, as at 2018, there were over 160 ethnic groups containing more than 100 people living in New Zealand. Moreover, 27.4% of those counted in the 2018 Census were born overseas.

5.73. As noted in chapter 1, we met on three occasions with Kāpuia during our work. We also met with groups from different communities within New Zealand: faith-based, ethnic, professional and other groups. Three points of particular significance emerged from these discussions.

5.74. The first is that, although they support the need for intelligence and security agencies and want them to be effective (especially given their own perceived vulnerability), some communities simply do not trust the Agencies. This mistrust may be rooted in their earlier lived experience in countries where the police and security forces are aligned with oppressive regimes. For others, however, it is a perception based on their experience in New Zealand. They see any engagement with the Agencies as one-way: they provide information or express their views but receive little or no feedback or indication that their input has had any effect. They may well be told that the Agencies are not free to share information with them. Overall, they feel ill-informed about the work of the Agencies and consider that no genuine dialogue occurs. As it was put to us, there has been "a history of engagement misalignment".[266] Obviously, these reactions are not conducive to further engagement with the Agencies by these communities.

5.75. The second and related point is that, without trust, the Royal Commission's desire to see an engaged and informed public discourse about national security issues and a commitment on the part of the public to the work of the Agencies will not be fulfilled. Building trust is a prerequisite to open and constructive discussion. This may require the Agencies to give the public more information about their activities than has been their practice to date, although, as noted, the Agencies have taken steps to be more open with the public about their work. We return to the issue of greater dissemination of information about the work of the Agencies when we discuss oversight.

5.76. The third point is that building trust requires the Agencies to operate in a way that reflects the diverse and multi-cultural nature of New Zealand society. This has implications both for the make-up of the Agencies (ie, those they employ) and the way they carry out their work. 'Diversity' is not simply a matter of race, gender or sexual orientation, it also encompasses matters such as age, educational background, socio-economic status, lived experience and other factors that affect a person's world view. Further, reflecting New Zealand's diversity is not simply a matter of employing people from diverse backgrounds, although that is an important step. Rather, it requires that a diversity of views is reflected in deliberative and decision-making processes throughout the Agencies.

5.77. We acknowledge that the Agencies have been working to increase the diversity of their workforces and their outlook and practices. In particular, in March 2018, the Agencies launched a joint diversity and inclusion strategy for 2017–2020, in response to workforce data showing low representation of women in technical, operational and middle management roles, as well as limited ethnic diversity generally. The aim of the strategy was to attract, retain, develop, progress and increase the number of women, Māori, Pasifika and other ethnic groups at all levels of the Agencies.

[265] Stats NZ "Ethnic group summaries reveal New Zealand's multicultural make-up" (3 September 2020).
[266] Submission from the Federation of Islamic Associations of New Zealand.

5.78. This was followed up in July 2021 with the refreshed *Diversity and Inclusion Strategy 2021–2025*,[267] which focuses on growing consistent diversity and inclusion capability across all leaders, from team leaders through to executive level. One specific initiative is the development of a targeted diversity and inclusion learning programme for leaders and staff across four core domains: language and culture, health and well-being, values and ethics, and inclusion.

5.79. While these efforts are commendable, our consultations and observations indicate that much is still to be done to achieve true diversity and inclusion within the Agencies. Research suggests that diversity and inclusion have tangible benefits for organisational performance. For example, a 2018 study of over 1,700 companies in eight countries found a relationship between diversity and innovation outcomes in all countries examined and suggested that "diversity represents a tangible missed opportunity and significant potential upside".[268] This has particular importance for the Agencies, given the work they do and the powers they possess.

5.80. The Intelligence and Security Committee of the United Kingdom Parliament captured an important practical reason for diversity within intelligence and security agencies in its report entitled *Women in the UK Intelligence Community*:[269]

> This is not just an ethical issue: it is vitally important from an intelligence perspective … Logically, if all intelligence professionals are cut from the same cloth, then they are likely to share 'unacknowledged biases' that circumscribe both the definition of problems and the search for solutions. Diversity should therefore be pursued not just on legal or ethical grounds – which are important in themselves – but *because it will result in a better response to a range of threats that we face to our national security*.

The Agencies accept this.

5.81. In addition to producing better outcomes by reducing or eliminating problems such as 'group think', true diversity and inclusion within the Agencies' workforces will help to meet the problem of lack of trust described in paragraphs [5.74–5.76]. Intelligence and security agencies that better reflect the communities they are charged with protecting are likely to have a greater understanding of, and be more responsive to, the concerns of those communities and, thereby, gain their trust and confidence.

5.82. Overall, we see a diverse and inclusive workforce within the Agencies as part of the process of facilitating effective democratic oversight.[270]

5.83. For completeness, we should note that there are impediments to recruiting people from diverse backgrounds to intelligence and security agencies generally.

- First, people from diverse backgrounds may not apply for jobs with intelligence and security agencies because they view such agencies as unsympathetic to the concerns of minority communities or they think they have little chance of being appointed. So, some degree of

---

[267] Government Communications Security Bureau and New Zealand Security Intelligence Service *Diversity and Inclusion Strategy 2021–2025* (online, no date).

[268] Rocio Lorenzo and Martin Reeves, "How and Where Diversity Drives Financial Performance", *Harvard Business Review* (online, 30 January 2018).

[269] Intelligence and Security Committee of Parliament *Women in the UK Intelligence Community* (2015) at 1-2 (emphasis added). This passage was quoted the committee's later report, *Diversity and Inclusion in the UK Intelligence Community* (2018) at 7. That later report outlines the business case for diversity and inclusion in the intelligence and security agencies: see especially pp 9–11. The Canadian National Security and Intelligence Committee of Parliamentarians has also undertaken a baseline assessment of diversity and inclusion in the Security and Intelligence Community within Canada.

[270] Intelligence and Security Act 2017, s 17(d).

self-selection may occur. Responses of this type came through in our consultations. This is an area the Agencies are working on.

- Second, recruits will need security clearances to enter secure facilities and see classified information. To obtain a security clearance in New Zealand, a person must hold at least a residence class visa and have a checkable history of up to 15 years. The vetting process for obtaining clearances can take between 2 and 12 months for complicated clearances. This, by its nature, can hinder the recruitment of some immigrants and refugees if the applicants do not have the required minimum checkable history for vetting.[271] This difficulty is exacerbated by over-classification of government information, which remains a problem.[272]

5.84. There is limited scope for addressing issues of this type through the ISA. The Public Service Act 2020, to which the Agencies are subject, places obligations on public service leaders and chief executives to develop a workforce that reflects the diversity of the society it serves and foster workplaces that are inclusive of all groups. Nevertheless, we think s 3(c) and s 17 should be amended to make it clear that the Agencies must, when performing their functions, act in a way that recognises and reflects the multi-cultural and diverse nature of modern New Zealand society. New Zealanders, whether citizens or permanent residents, come from many different cultures. They all have a stake in the preservation of New Zealand as a free, open and democratic society, yet many feel vulnerable because of their distinctive ethnicity, cultural or religious beliefs. A statement of principle such as we suggest will not result in immediate change. It will, however, emphasise – to the Agencies, to communities (especially those who feel vulnerable) and to New Zealanders more generally – the importance Parliament places on recognising the diversity of New Zealand's people and on integrating that recognition into intelligence and security structures and the work the Agencies carry out.

RECOMMENDATION 04

Amend section 3(c) (Purpose) of the Intelligence and Security Act 2017 to give effect to te Tiriti o Waitangi/the Treaty of Waitangi and the multi-cultural and diverse nature of New Zealand society, along the following lines (with corresponding amendments to section 17 (General duties)):

> The purpose of this Act is to protect New Zealand as a free, open, and democratic society by—
>
> (c) ensuring that the functions of the intelligence and security agencies are performed—
>
> (i) in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; and
>
> **(ii) in accordance with the Crown's responsibilities to Māori under te Tiriti o Waitangi/the Treaty of Waitangi;**
>
> **(iii) in a manner that reflects New Zealand's multi-cultural and diverse society;**

[271] See, for example, *Diversity and Inclusion in the UK Intelligence Community* (2018) at 30; Edward Lucas "The Spycraft Revolution – Changes in technology, politics, and business are all transforming espionage. Intelligence Agencies must adapt – or risk irrelevance" *Foreign Policy* (online, 27 April 2019).

[272] Inspector-General of Intelligence and Security *A review of the New Zealand Security Classification System* (August 2018). We return to this issue in chapter 10.

> **(iv) in the performance of its operational functions, independently, and impartially;**
>
> (iv) with integrity and professionalism; and
>
> (v) in a manner that facilitates effective democratic oversight;

Section 19: Activities not to limit freedom of expression

5.85. As noted in chapter 2, the Royal Commission considered s 19 could be interpreted in a way that hindered the Agencies' ability to undertake legitimate target discovery activities. The Royal Commission recommended the section be given further consideration, which we do below.

5.86. To reiterate, s 19 provides:

> **Activities of intelligence and security agency not to limit freedom of expression**
>
> The exercise by any person in New Zealand or any class of persons in New Zealand of their right of freedom of expression under the law (including the right to advocate, protest, or dissent) does not of itself justify an intelligence and security Agency taking any action in respect of that person or class of persons.

5.87. The prohibition in the section is against an Agency 'taking any action'. The Royal Commission illustrated what it saw as the problem with the section by reference to the following example:

- some people, including those on the far right, use websites and online forums to spread or receive divisive and hateful rhetoric; and
- some of those people may be potential terrorists and analysis of what is said on those websites and forums might enable them to be identified; but
- little of the divisive and hateful rhetoric found on such websites and forums is contrary to the law.

The Royal Commission considered it was at least arguable that any collection and analytical work carried out by the Agencies regarding such websites and forums would breach s 19.

5.88. We discuss the issue under three headings: legislative background, the approaches of comparable jurisdictions and our assessment.

Legislative background

5.89. When first enacted, the New Zealand Security Intelligence Service Act 1969 (NZSIS Act) did not contain a provision comparable to s 19. However, in 1977 the NZSIS Act was amended to include (among other things) a new s 4(2) stating it was not the function of the Security Intelligence Service:[273]

> (a) To enforce measures for security; or
>
> (b) To institute surveillance of any person or class of persons by reason only of his or their involvement in lawful protest or dissent in respect of any matter affecting the Constitution, laws, or Government of New Zealand.

[273] New Zealand Security Intelligence Service Amendment Act 1977 (1977 No 50), s 3(2).

This resulted from an amendment made as the Amendment Bill went through the House.[274] The Bill was controversial at the time, leading to large protests outside Parliament.[275]

5.90. It is relevant to note that this amendment was made more than a decade before the enactment of the New Zealand Bill of Rights Act 1990 (NZBORA). The relevance of this is that NZBORA protects several relevant rights, for example, freedom of expression,[276] freedom of peaceful assembly[277] and freedom of association.[278] The rights and freedoms in NZBORA "may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".[279]

5.91. The NZSIS Act was amended again in 1999 to repeal s 4(2) and to add the following provision as s 2(2):[280]

> Nothing in this Act limits the right of persons to engage in lawful advocacy, protest, or dissent in respect of any matter, and, accordingly, the exercise of that right does not, of itself, justify the Security Intelligence Service in instituting surveillance of any person or entity or any class of person or entity within New Zealand.

5.92. In August 2016 the New Zealand Intelligence and Security Bill was introduced. The departmental disclosure statement noted that the Bill "continues existing protections around political neutrality, lawful advocacy, protest, and dissent".[281] On introduction, clause 22 read:[282]

> **Limitation on collecting intelligence within New Zealand**
>
> (1) Nothing in this Act limits the right of persons to engage in lawful advocacy, protest, or dissent in respect of any matter.
>
> (2) The exercise of the right in subsection (1) does not, of itself, justify an intelligence and security agency collecting intelligence on any person who is in New Zealand or any class of persons who are in New Zealand.

5.93. The departmental report on the Bill referred to the concern of some submitters at the reference to 'lawful' protest and that this limitation unduly narrowed the protection provided. Submitters made two suggestions that were accepted by the Department of the Prime Minister and Cabinet.[283]

- The Legislation Design and Advisory External Subcommittee considered that the term 'freedom of expression' was a better way of capturing what was intended to be protected by clause 22.
- The Inspector-General of Intelligence and Security was concerned over the change in wording in the comparable clause from 'instituting surveillance' in the NZSIS Act, to

---

[274] New Zealand Security Intelligence Service Amendment Bill 1977 (73-1).

[275] Ministry for Culture and Heritage "Security Intelligence Bill protests, 1977" (updated 16 July 2014) New Zealand History <nzhistory.govt.nz/media/photo/security-intelligence-bill-protests>.

[276] New Zealand Bill of Rights Act 1990, s 14.

[277] Section 16.

[278] Section 17.

[279] Section 5.

[280] New Zealand Security Intelligence Service Amendment Act (No 2) 1999 No 91.

[281] *Departmental Disclosure Statement: New Zealand Intelligence and Security Bill* (15 August 2016) at 3.

[282] New Zealand Intelligence and Security Bill 2016 (158–1).

[283] Department of the Prime Minister and Cabinet *New Zealand Intelligence and Security Bill: Departmental Report to the Foreign Affairs, Defence and Trade Committee* (December 2016) at [304]–[322].

'collecting intelligence' in the Bill because this could be construed as limited to collecting intelligence pursuant to an intelligence warrant. The Inspector-General considered that lawful advocacy, protest and dissent do not in themselves justify the Agencies taking any action at all and suggested the Bill should be reworded to capture this.[284]

5.94. In response to questions from the select committee on this issue, the Department of the Prime Minister and Cabinet suggested that the revised wording recognised 'freedom of expression' in an unbounded way and the reference to the right to advocate, protest or dissent was not an exhaustive expression of what was to be protected. Furthermore:[285]

> Nothing in the Bill, including the definition of "national security", limits the right to freedom of expression. To the extent that an act is recognised by the law currently as a protected act of freedom of expression in accordance with section 14 of the New Zealand Bill of Rights Act 1990, the agencies will not be able to take any action on the basis of that act alone.

5.95. Following deliberations in the Foreign Affairs, Defence and Trade Select Committee, the clause was amended and became s 19 as it currently stands. Similar provisions are found in s 5(5) of the Terrorism Suppression Act 2002, s 3B of the Maritime Crimes Act 1999 and s 5 of the Maritime Security Act 2004. The effect of the provisions in these Acts is rather different from s 19, however, because they prevent protest, advocacy or dissent from being treated as an ingredient of an offence.

Approach taken in other comparable jurisdictions

5.96. Australia and Canada have included protections similar to s 19 in their intelligence and security legislation. Australia, which does not have a Bill of Rights at the federal level, has a legislative provision limiting the functions of the Australian Security Intelligence Organisation in the following terms:[286]

> **17A Act not concerned with lawful dissent etc.**
>
> This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly.

5.97. Canada, which does have an equivalent to NZBORA in the Canadian Charter of Rights and Freedoms, enacted in 1982, also protects freedom of speech and the right to protest in its intelligence and security legislation. At paragraph [5.31], we quoted the definition of 'threats to security' from the Canadian legislation. That definition ends with the words:

> ... but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

5.98. Furthermore, the Security of Canada Information Sharing Act 2015 gives certain federal bodies the ability to disclose Canadians' personal information to other government institutions that have mandates or responsibilities relevant to the detection, identification, analysis, prevention, investigation or disruption of "activities that undermine the security of Canada".[287] This term

---

[284] Above n, at [312].
[285] Department of the Prime Minister and Cabinet *New Zealand Intelligence and Security Bill: Information Requests Arising from the Committee's 8 December 2016 Meeting* (12 December 2016) at 2.
[286] Australian Security Intelligence Organisation Act 1979 (Cth).
[287] Security of Canada Information Disclosure Act SC 2015, c 20, s 3.

includes activities that undermine the sovereignty, security or territorial integrity of Canada, such as espionage, covert foreign-influenced activities, terrorism and significant interference with critical infrastructure. Section 2(2) of the Act provides:

> For the purposes of the Act, advocacy, protest, dissent or artistic expression is not an activity that undermines the security of Canada unless carried on in conjunction with an activity that undermines the security of Canada.

5.99. Finally, we note that the US Foreign Intelligence Surveillance Act 1978 provides for the issue of electronic surveillance authorisations where the target of the surveillance is a foreign power or an agent of a foreign power, provided that "no United States person may be considered an agent of a foreign power solely on the basis of activities protected by the first amendment to the Constitution of the United States".[288] The context of the Act addresses foreign intelligence surveillance and places constraints on electronic surveillance of United States citizens. It therefore operates as a limitation on the activity of electronic surveillance.

Our assessment

5.100. We note that s 19 and its impact on the Agencies' ability to identify potential threats was raised by some who we consulted. In addition, as part of our public engagement process, we asked whether the Agencies should be able to investigate people who express extremist views in exercising their right of free speech. Most submitters and those we consulted agreed s 19 should not be, or is not, a barrier to identifying potential threats. At the same time, however, there was broad acknowledgement that members of the public should not be subject to investigation by the Agencies simply for expressing disagreement with accepted norms of society or particular government policy decisions.

5.101. In strictly legal terms, s 19 may be unnecessary. As discussed above, the original version of what is now s 19 was enacted in 1977, well before the enactment of NZBORA. Today, however, the Agencies are under a duty when performing their functions to act "in accordance with New Zealand law and all human rights obligations recognised by New Zealand law".[289] Section 14 of NZBORA, which protects freedom of expression, is part of New Zealand law that the Agencies must honour. This means that removing s 19 from the ISA would not meet the problem that the Royal Commission identified as it arises under NZBORA in the same way as it does under s 19.

5.102. The main difficulty with provisions such as s 19 of the ISA (or, in the present context, s 14 of NZBORA) is that it may not be obvious to an intelligence and security agency whether or not protected advocacy, protest or dissent is occurring in conjunction with behaviours that undermine national security until it has investigated the position. In considering whether s 19 does prevent an agency from investigating the position in appropriate cases, it is important to be clear about two things: what s 19 protects and what it prohibits.

5.103. In relation to what s 19 protects, the heading to the section reads: "Activities of intelligence and security agency not to limit freedom of expression". That indicates what the section is about. The section then goes on to refer to the exercise of the "right to freedom of expression under the law". But the right of freedom of expression protected by NZBORA is not absolute. The courts have accepted it is a right that may be limited in a free and democratic society under s 5 of NZBORA.[290] So, 'expression' may, in some contexts, be a basis for criminal (or civil) liability.

---

[288] Foreign Intelligence Surveillance Act 50 USC, §§ 1801 et seq., s 105.

[289] Intelligence and Security Act 2017, s 17(a).

[290] See, for example, *Brooker v Police* [2007] NZSC 30, [2007] 3 NZLR 91 and *Morse v Police* [2011] NZSC 45, [2012] 2 NZLR 1.

5.104. Some speech may be so violent, hateful and extreme and, in particular circumstances, so obviously provocative that it would not be protected under NZBORA. However, as just noted, in the context of an organised protest, it will not always be self-evident to outside observers whether demonstrators are simply exercising their freedom of expression, which is protected, or whether they have crossed the boundary into unprotected areas, so that their activities justify the attention of the Agencies. Whether a protest is simply a protest or involves as well activities that justify the attention of the Agencies will have to be determined in the particular circumstances of the protest. That will depend on factors such as the objectives of the protest, its nature, the surrounding circumstances and the way the protest is conducted. Clearly, given s 19 and their obligation to act in a politically neutral way,[291] the Agencies should take a cautious approach in such circumstances. But in our view, s 19 does not prevent an Agency from investigating protesters if there are circumstances that raise a legitimate question as to whether protesters are considering activities that would threaten national security.

5.105. Turning to what it prohibits s 19 prohibits an Agency from "taking any action in respect of that person or class of persons" (ie, the person(s) exercising their right of free expression). That would not, in our view, prevent an Agency from sending someone along to a protest to observe it if there was some indication that there was more to the protest. Nor would it prevent someone from an Agency entering an internet chat room known to host extremist and violent content to see what was happening and, if someone of interest was identified, looking into that person's background.

5.106. In summary, the point of s 19 is that the Agencies should not limit people's freedom of expression. Given that the right of freedom of expression is qualified, not absolute, the Agencies are, in our view, entitled to make an assessment that some types of expression in particular circumstances justify their interest, although they should adopt a cautious approach. We therefore consider that there will be circumstances where the Agencies may legitimately investigate situations where, for example, violent extremist views are being expressed without, in doing so, breaching s 19. We acknowledge, however, that that the issue is difficult and requires careful judgment by the Agencies.

5.107. The result is that we consider that s 19 should be retained in the ISA. Section 19 serves an important function in that it highlights the vital importance of freedom of expression to maintaining a free, open and democratic society. The fact that it was included in the ISA reflects the democratic paradox referred to in chapter 1 – we see intelligence and security agencies as necessary and important for our protection and decision-making but worry about the extent and exercise of their powers. Even though s 19 is, in a sense, unnecessary, we consider it serves as an important statement of principle, as a significant reminder to the Agencies and as a reassurance to the public. Removing s 19 will not remove the difficulty that the Agencies face as it will remain under s 14 of NZBORA.

RECOMMENDATION 05

Retain section 19 (Activities of the intelligence and security agency not to limit freedom of expression) of the Intelligence and Security Act 2017 without amendment.

[291] Intelligence and Security Act 2017, s 18(a)(iii).

SECTION 03

Information collection for intelligence and security

CHAPTER 06

How intelligence and security agencies gather information

Introduction

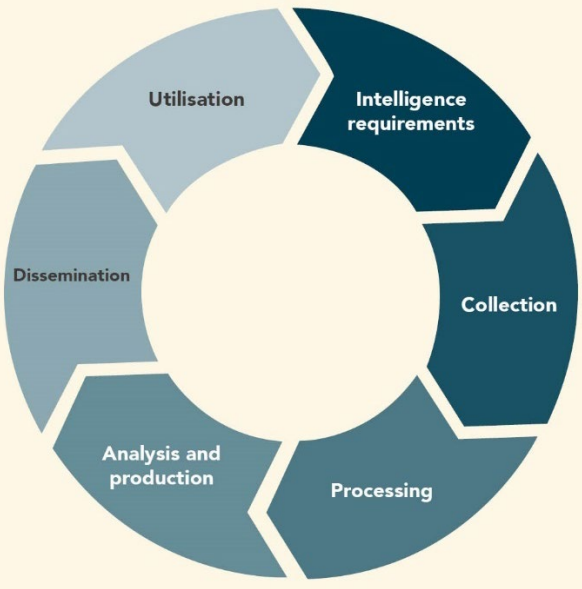
6.1. This chapter provides an overview of how the two intelligence and security agencies the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) (referred to in our report as 'the Agencies') can gather information.

6.2. We then consider matters arising from that information gathering, in particular, the distinction between lawful and unlawful activities, open-source information, targeted and non-targeted activities, the relevance of nationality and the significance of retention and disposal provisions.

The intelligence cycle

6.3. We discussed the state's need for intelligence in chapter 2 and outlined the intelligence function. Diagram 1 summarises the intelligence cycle. This involves developing unrefined data into intelligence products for use by government and agency decision-makers. The process is circular, but movement between stages does not always follow this progression.

Diagram 1: Intelligence cycle



6.4. Each element of the cycle is briefly described below.

- **Intelligence requirements**: A government agency will formulate intelligence plans and questions (also called requirements) that focus an intelligence gathering exercise and take into consideration the national security intelligence priorities (as discussed in chapter 5).
- **Collection**: Collection is the process of gathering information to respond to the intelligence requirements.
- **Processing**: Processing turns the collected data into a readable format (eg, through translation).
- **Analysis and production**: Analysis turns the processed information into intelligence that can inform agency or government decision-making.
- **Dissemination**: Dissemination involves getting the intelligence product to the agencies or government decision-makers that need it.
- **Utilisation**: Utilisation refers to the processes by which agencies and others use information, including to inform decision-making.

Gathering information

6.5. Good information is key to good intelligence. As noted in chapter 2, intelligence may be simply processed information, especially information that has been obtained secretly, or it may be the product of an analysis of a range of information, whether publicly available, obtained through government sources such as diplomatic reporting, secretly obtained or some combination of the three.

6.6. As a product, intelligence seeks to help decision-makers understand and interpret what is or has been happening and to provide a basis for assessing what is likely to happen in the future. If it is to be relied on, the information, and any analysis or assessment of it, needs to be as accurate and comprehensive as possible.

6.7. In fulfilling their statutory functions, the Agencies can gather information in a variety of ways. They can:

- collect publicly available information just as anyone else can, eg, from sources such as media outlets; academic, professional and special-interest journals; government and corporate publications; publicly available databases (eg, electoral rolls and business directories) and publicly accessible social media pages.[292] We refer to this as open-source information. Digitisation has meant that the amount of good-quality, open-source information available has been growing exponentially for some time and will continue to grow
- obtain information from foreign partners
- obtain information by covert means (eg, undercover work carried out through assumed personal identities or through corporate structures that disguise their real purpose)[293]
- collect other information when they are permitted to do so, such as:

[292] The collection of publicly available information is subject to a ministerial policy statement. See Ministerial Policy Statement "Publicly available information" (1 March 2022).

[293] Intelligence and Security Act 2017, ss 21–45.

- under **warrants**, granted by either the Minister and a Commissioner of Intelligence Warrants in the case of New Zealand citizens and permanent residents[294] or the Minister alone in other cases, to do things that would otherwise be unlawful (like intercepting mobile phone communications or accessing information infrastructures)[295]
- by **approvals**, granted by the Minister and a Commissioner of Intelligence Warrants in the case of New Zealanders or the Minister in other cases, to access restricted information, which includes tax information held by Inland Revenue, images from driver licences, adoption information and information relating to the national student numbers assigned to tertiary students by the Secretary of Education[296]
- by **directions** made by a Director-General of one of the Agencies under general, time-limited **approvals** granted by the Minister and a Commissioner of Intelligence Warrants to obtain business records held by either telecommunications companies or banks and other financial services providers, which the relevant entity is obliged to provide[297]
- by **direct-access agreements** between the Minister responsible for one of the Agencies and the Minister responsible for a public sector agency holding any of the databases specified in Schedule 2 of the Intelligence and Security Act 2017 (ISA). Those databases relate to matters such as births, deaths and marriages / civil unions; citizenship; immigration; customs and financial intelligence[298]
- by making a general **request for information** from a public or private agency, which is not required to provide the information and may, if it wishes, refuse the request[299]
- by receiving **unsolicited information**.

6.8. During our review, we received submissions and comments about these various methods of obtaining information, which we will discuss in more detail in this and later chapters of the report. In particular, we discuss issues in relation to:

- open-source information in this chapter
- warrants in chapter 7
- direct access agreements in chapter 9
- business records directions, approvals to obtain restricted information and information provided voluntarily in chapter 9
- information provided by foreign partners in chapter 10.

Lawful/unlawful distinction

6.9. There is much the Agencies can do in performing their functions without seeking warrants to use intrusive powers. One example is the function of the GCSB in relation to providing information assurance and cyber-security activities and protecting the security and integrity of communications and information infrastructures of importance to the government. Much of GCSB's activity in the

[294] Section 53.
[295] Sections 46–117.
[296] Sections 134–142.
[297] Sections 143–155.
[298] Sections 124–133.
[299] Intelligence and Security Act 2017, ss 120–122.

performance of this function takes place with the consent of the entities concerned and does not require a warrant.

6.10. Nevertheless, there will be circumstances where the GCSB requires a warrant for activities in relation to its cyber-security functions. So, when must an Agency obtain a warrant to undertake particular activities? The essential (but not complete) answer is: when the activities would be unlawful without a warrant.

6.11. Part 4 of the ISA deals with warrants.[300] The purpose of Part 4 is to:[301]

> … establish an authorisation regime for the intelligence and security agencies that–
>
> (a) authorises as lawful the carrying out of an activity by an intelligence and security agency that would otherwise be unlawful, if certain criteria are satisfied; and
>
> (b) confers on an intelligence and security agency specified powers for the purpose of giving effect to an authorisation.

6.12. Sections 48 and 49 of the ISA give effect to this purpose.

- Section 48 provides that an Agency may, in performing its functions or duties or exercising its powers, carry out a lawful activity without an authorisation.
- Section 49(1) provides that an Agency may only carry out an otherwise unlawful activity if that activity is authorised.

6.13. Section 49(3) provides that an Agency may carry out authorised activities lawfully "despite anything to the contrary in any other enactment". We consider that reference to "any other enactment" means activities that are unlawful under the ISA itself cannot be authorised. An example is the use of vetting information for purposes other than those set out in s 220.

6.14. The distinction between activities that are unlawful and those that are lawful is crucial to the Agencies' power to act and to the operation of the warranting regime.

6.15. However, there is an issue as to the scope of the word 'unlawful'. An activity that constitutes an offence is unlawful and requires authorisation under a warrant. Similarly, some activities that would not amount to offences but would be civil wrongs are also unlawful and require authorisation under a warrant. An example of this is trespass. If an NZSIS officer wanted to go on to someone's property without their permission to look through a garage window to identify the colour and make of the vehicle parked inside, the officer would require a warrant, even though going onto the property without permission would not (in the absence of an earlier warning) be an offence.

6.16. But do all civil wrongs trigger the 'unlawfulness' criterion? For example, if an Agency obtained publicly accessible data in which there was no privacy interest from websites in a way that breached the website's terms and conditions, would that meet the unlawfulness criterion? Moreover, is it always the case that the Agencies should be able to access without a warrant information that is publicly available and accessible to members of the public? This raises the question of whether the focus should be solely on lawfulness or whether propriety is also relevant in this context.

---

[300] Part 4 is entitled "Authorisations". That term is defined in s 47 to include intelligence warrants, removal warrants, practice warrants, and very urgent authorisations granted by the Director-General of an intelligence and security Agency under s 78.

[301] Intelligence and Security Act 2017, s 46.

6.17. Section 17(a) of the ISA requires the Agencies to act "in accordance with New Zealand law and all human rights obligations recognised by New Zealand law". This includes the New Zealand Bill of Rights Act 1990 (NZBORA). Section 21 of NZBORA provides that everyone has the right to be secure against unreasonable search and seizure. In the main, s 21 protects people's privacy interests.[302] The courts have held that the lawfulness of a search does not automatically determine whether the search was reasonable – a search that is lawful may nevertheless be unreasonable for s 21 purposes.[303] While this is not directly relevant in the present context, a similar principle applies to the Agencies.

6.18. To give a hypothetical example, assume the Minister issues a ministerial policy statement providing guidance to the Agencies about investigations and operational activities in relation to sensitive category individuals. It states that Agencies should develop and implement appropriate operational policies and approval processes. An Agency becomes concerned about the activities of a sensitive category individual and that person's associates. The Agency obtains warrants to exercise intrusive powers in respect of several of the individual's associates to obtain information about them but also in the hope of learning something about the individual. The Agency's actions may be lawful[304] but, if the effect was to undermine the Minister's guidance in relation to sensitive category individuals, they may be seen to be unreasonable.

6.19. Accordingly, the concepts of 'necessity' and 'proportionality', which apply in the warranting context, are also relevant in relation to open-source information, as is confirmed by the ministerial policy statement on publicly available information.

Open-source information

6.20. Like others, the Agencies are free in principle to collect publicly available information – it is a lawful activity for which a warrant would not generally be required. Our public engagement highlighted divergent views on the Agencies' collection of publicly available information. We asked participants whether they would feel more or less protected if the Agencies collected information that is openly available on the internet (including about them or their communities) to help identify potential risks and threats to Aotearoa New Zealand unknown to the Agencies. The respondents were evenly split. Those who considered they would feel more protected cited a range of reasons, including that harnessing publicly available information could be a potentially powerful tool to better assess information and identify potential threats. Those opposed emphasised the need to protect privacy and expressed concerns about mass state surveillance, particularly as dissenting ideas and perspectives could be politicised or viewed as risks and threats.

6.21. This highlights an interesting contrast in perspectives. Intelligence and security agencies that acquire data in bulk from public sources are likely to see the acquisition as involving low privacy interests, at least up until the stage that specific data are selected for detailed analysis. However, from the perspective of at least some members of the public, the agencies' acquisition of bulk data from public sources will be perceived as state surveillance, irrespective of any subsequent analysis. This may, in turn, affect the agencies' social licence.

---

[302] *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [10] per Elias CJ and at [161] per Blanchard J.

[303] *R v Williams* [2007] 3 NZLR 207 (CA) at [24].

[304] Depending on the precise circumstances, there may be an issue about whether the Agency had met its duty of candour, but we ignore that for present purposes.

6.22. In our view there are, or should be, exceptions to the Agencies accessing publicly available information without a warrant. We will focus on three.

- First, there may be information that is available to the public on the internet, but only because it has been improperly hacked from a confidential database and then published. Should a state agency be able to collect such information freely, or should the fact that it was made public only because it was improperly obtained and published mean that the Agencies should not access it unless they have a warrant to do so?
- Second, we referred in chapter 2 to a company that scanned the internet by automated means to obtain publicly available images of peoples' faces so that its facial recognition technology could be applied to them to create biometric identifiers. The company held a database of billions of images with their biometric identifiers and sold access to this database to a variety of organisations, including law enforcement agencies. Should the Agencies and other state entities be permitted to access data of this type without seeking a warrant?
- Third, many websites have terms and conditions that prohibit scraping (the process of using algorithms to extract content and data from a website). It is also common for websites to attempt to prevent scraping by building defences into their websites' technology. If an Agency scrapes such websites to obtain information that is publicly accessible and that raises no (or low) privacy interests but has done so in breach of the websites' terms and conditions or has bypassed their defences in some way, does it act unlawfully for the purpose of the warranting provisions?

6.23. Before addressing these issues, we note an emerging area of concern internationally in relation to commercially and publicly available data. As will be apparent from the discussion of technological developments in chapter 2, private-sector companies are increasingly attempting to take advantage of the data explosion that has occurred in recent times, and intelligence and security agencies in Europe and elsewhere have sought to benefit from their activities. In a recently published monograph,[305] Thorsten Wetzling and Charlotte Dietrich claimed that European intelligence services are using commercially and publicly available data more frequently, to the point that there has been a paradigm shift in intelligence practice.

6.24. Wetzling and Dietrich give an example of a private sector company that has access to a near real-time database of billions of geolocation signals from cell phones. The company sells a subscription service to law enforcement agencies, which enables the agencies to obtain cell phone location data in relation to either locations or devices of interest. The company acquires the data from the third-party applications on smart phones that have permission to collect users' locations. The app owners sell that information to third party advertisers or data processors. The data gets on-sold and amalgamated, to form databases of the sort described. Consequently, the traditional focus of regulatory efforts on intelligence and security agencies' use of compulsion or direct access agreements to obtain information may no longer reflect what is increasingly happening, and further regulation of the use of open-source material may be needed.

[305] Thorsten Wetzling and Charlotte Dietrich *Disproportionate use of commercially available and publicly available data: Europe's next frontier for intelligence reform?* (Think Tank at the Intersection of Technology and Society, November 2022).

Hacked and leaked data sets

6.25. There have been several recent incidents in New Zealand of datasets containing patients' private medical information being hacked from medical providers and uploaded to the internet where it is publicly available.[306] Internationally, there have been large-scale leaks of confidential banking and personal information.[307] As noted in chapter 2, there are companies that aggregate hacked and leaked datasets and sell access to them.

6.26. As we understand it, the Agencies' current practice is to seek warrants to access hacked and leaked data. The Agencies asked us to consider whether they should be able to access such datasets without warrant where it is publicly available information.

- It could be argued that accessing a dataset that has been unlawfully hacked from a private source and then published on the internet is unlawful, on the basis that the access is akin to receiving stolen property.[308] There are difficulties with such an argument, however, particularly where the leaked dataset is widely accessed. The better view may be that while the initial hacking was unlawful and would constitute an offence, subsequent access to information in the dataset (as distinct from acquiring the dataset) by a third party on a platform to which the public have access is not unlawful.
- Even if a third party's subsequent access to a hacked or leaked dataset is lawful, does that necessarily mean that the Agencies (or indeed other state agencies) should be entitled to access such datasets without warrant or are there other relevant interests that mean that the Agencies should only access them with a warrant?

6.27. As discussed earlier,[309] the oversight provisions in the ISA make it clear that oversight extends to both the legality and the propriety of the Agencies' activities. Accordingly, an act that is lawful may, despite that, be improper (or lack propriety). While it may not be the case for all information in hacked or leaked datasets, there is a strong argument that propriety considerations arise where hacked or leaked datasets contain confidential personal information, such as medical records, banking information and other confidential personal data. People are likely to have a reasonable expectation of privacy in confidential personal information of this type.

6.28. In such instances, we consider the Agencies should only be able to acquire and use the information under the authority of a warrant. The Minister and Commissioner considering the warrant application can consider and address the relevant privacy interests, which may mean rejecting an application or issuing a warrant that is subject to limitations or conditions intended to protect legitimate privacy interests. Addressing the issue of access by the Agencies solely on the basis of a lawful/unlawful criterion (which may, in any event, be contentious) is, we believe, unsatisfactory.[310]

6.29. This is consistent with the approach the Agencies take to overseas partners' confidential information that becomes publicly available as a result of the publication of hacked or leaked datasets. Foreign partners will often continue to treat information that becomes public through

---

[306] In August 2019, the Ministry of Health was informed of an illegal cyber intrusion of the digital information systems of Tū Ora Compass Health (a primary health care network for the Wellington, Porirua, Wairarapa and Kāpiti areas), with the data covering nearly 1 million patients.

[307] For example, the 2014 hack and leak of Sony Pictures Entertainment internal financial information and the 2022 hack of personal information of OPTUS mobile phone customers.

[308] Crimes Act 1961, s 246.

[309] See in particular chapter 4.

[310] The Agencies may receive information from hacked or leaked datasets from foreign partners. The Agencies consider such unsolicited information to be lawfully obtained, so no warrant is required.

unauthorised leaks as confidential. Where partners, such as New Zealand, hold such information, they will respect this approach. This is on the basis that a leaked publication does not change the confidential character of the information, even though it is publicly available on the internet. It is difficult to see why a different principle should apply to the confidential information of private citizens.

6.30. We acknowledge that requiring the Agencies to obtain warrants in relation to hacked and leaked datasets could impose a constraint on them that their adversaries in autocratic states do not face. But that is a challenge that intelligence and security agencies in democracies inevitably face. In practice, if there is genuine intelligence value in the information the Agencies wish to use, a warrant is likely to be granted, and the constraint would, in effect, be no more than administrative.

Use of technological tools to produce biometric data from publicly and commercially available data

6.31. We return to the example of the company that scraped the internet for people's images, created facial recognition biometrics for each image and then sold access to the database to law enforcement and other agencies. While people sitting at computer terminals could go through publicly accessible platforms and copy people's images and, in this way, gradually build up a database, collection and analysis on the scale referred to has been made possible only by the development of technological tools.

6.32. The ability to use technology to acquire, store and analyse large amounts of data affects the nature of the interests involved. The transformation of material such as images into valuable biometric identifiers – and into intelligence – fundamentally changes the character of the material. Generally, this process will result in new, more valuable information but also information that is more sensitive.

6.33. For example, despite doubts about its universal accuracy, facial recognition technology has been developed to the point that Police and other agencies in comparable jurisdictions can undertake instantaneous facial recognition by accessing a live CCTV feed and comparing images appearing on the feed with images in a database, which may identify persons of interest to them.[311] While Police officers on patrol may be able to recognise people who are being sought from photographs, the technology greatly outstrips human capabilities.

6.34. Obviously, such technologies have the potential to improve the efficiency and effectiveness of law enforcement, intelligence and security and other state agencies significantly. However, they also raise concerns about the 'surveillance state'. Efficiency and effectiveness are important, but so also are privacy and other human rights, as well as wider societal interests. A person's biometric data is inherently sensitive, including in a culturally specific way.[312]

6.35. The complexity and automated nature of the technology can make it difficult for people to challenge decisions, and the benefits of the technology can also be overstated. Incomplete data

[311] Nessa Lynch and Andrew Chen *Facial Recognition Technology: Considerations for use in Policing* (Independent Report commissioned by New Zealand Police, November 2021) at 37. See also Nessa Lynch, Liz Campbell, Joe Pursehouse and Marcin Betkier *Facial Recognition Technology in New Zealand* (The Law Foundation, November 2020).

[312] See, for example Office of Privacy Commissioner *Office of the Privacy Commissioner Position on the Regulation of Biometrics* (October 2021) and *Privacy Regulation of Biometrics in Aotearoa New Zealand: Consultation paper* (August 2022).

and the fallibility of human programming can lead to inaccuracy and bias (especially against women and ethnic minorities).

6.36. Moreover, the issues raised by these new technologies need to be considered against a broader background than simply the activities of intelligence and security agencies, given that the type of technological tools referred to are being considered or used by other state agencies and by the private sector. A comprehensive, coherent approach needs to be taken.

6.37. What does this mean in the context of the Agencies activities? In our view, the critical issue is not so much lawfulness or unlawfulness (which may be difficult to determine in any event), but rather the interests involved. By way of example, when people are in public spaces, typically, their faces are exposed, and images of them can readily be captured without their knowledge. If biometric data is developed from these images, the result can be a database of sensitive identifiers, which could be put to a variety of uses. In terms of privacy interests, and in terms of the exercise of other rights and freedoms, this could be highly intrusive. Consequently, the Agencies should seek warrants to access (or to generate) data of this type, reflecting the data's nature and sensitivity.

Breaching terms and conditions

6.38. What is the position where an Agency wishes to scrape a website contrary to its terms and conditions or to defeat its technological defence systems so that it can undertake scraping? Should the Agency need a warrant?

6.39. The issue of scraping contrary to terms and conditions has arisen in several cases in United States of America, a recent example being the *hiQ Labs, Inc v LinkedIn* litigation. LinkedIn's terms and conditions, which were expressed to apply to registered users and to visitors to the site, prohibited both unauthorised scraping and setting up accounts in false names. LinkedIn also set up technical impediments or defences to scraping activities. hiQ Labs evaded LinkedIn's technical defences and scraped data from LinkedIn's website, both directly and with the assistance of contractors, some of whom set up fake LinkedIn accounts. In the litigation, LinkedIn alleged first, that hiQ Labs had breached the United States Computer Fraud and Abuse Act 1986 by its unauthorised access to the website and second, that it was in breach of LinkedIn's terms and conditions.

6.40. In relation to the first claim, the United States Court of Appeals for the Ninth Circuit considered that hiQ Labs' scraping of LinkedIn's website for information from profiles that were visible to the general public did not constitute unauthorised access for the purposes of the Computer Fraud and Abuse Act, even though hiQ Labs had received a cease-and-desist letter from LinkedIn.[313] The Court noted that LinkedIn had no protected property interest in the information in the public profiles as users retained ownership over their profiles. It appears that LinkedIn issued the cease-and-desist notice to protect its own commercial interests in its subscribers' data, which it was proposing to monetise itself.

6.41. In relation to the breach of contract claim, the District Court held, in a later decision, that hiQ Labs had breached LinkedIn's terms and conditions by its scraping activities and its use of scraped data, as well as through its contractors' setting up of fake accounts. Ultimately the parties settled the litigation.[314]

---

[313] *HIQ Labs, Inc v LinkedIn Corporation* (2022) 31 F.4th 1180 (9th Circ.)

[314] The National Law Review "hiQ and LinkedIn Reach Proposed Settlement in Landmark Scraping Case" (Thursday December 8th 2022) volume XII, number 342.

6.42. Our view is that where the public have access to data on a website such as LinkedIn, the fact that its terms and conditions proscribe scraping does not mean an Agency's scraping of that publicly accessible data is unlawful for the purposes of the ISA. However, if the Agency then manipulated the data by, for example, developing biometric identifiers from images obtained from the site, that activity would require an authorisation, for the same reasons discussed in the preceding section.

Conclusion

6.43. We consider that the lawful/unlawful distinction should remain but that where lawfulness is uncertain, warrants should be sought.

6.44. Further, irrespective of lawfulness/unlawfulness, we consider that the acquisition of hacked and leaked datasets or sensitive datasets (such as biometric identifiers) developed from publicly available images or similar material by a third party should be authorised by warrants. Where the Agencies undertake the development of sensitive datasets themselves from publicly available material, they should be required to obtain a warrant or other form of authorisation. In respect of these classes of material, the lawfulness/unlawfulness test is difficult to apply and does not, by itself, adequately reflect the interests involved. These qualifications could be incorporated into the ISA or dealt with by way of ministerial policy statement.

6.45. Additionally, like the Privacy Commissioner, we note that the number of government agencies using and practicing open-source techniques has grown and agree with his questions about whether state accountability mechanisms have been able to keep up with the rapid changes in this area.[315]

RECOMMENDATION 06

Retain the lawfulness/unlawfulness criteria that govern the warranting framework in sections 48 and 49 (Authorisations) of the Intelligence and Security Act 2017, subject to the following qualifications.

a. If the lawfulness of a proposed activity by an intelligence and security agency in performing its functions, duties or powers is uncertain, a warrant to carry out the activity should be sought.

b. A warrant should be sought where the Agencies wish to obtain access to hacked and leaked datasets and sensitive datasets developed by third parties from publicly available material, such as facial images.

c. Where the Agencies seek to develop sensitive datasets themselves from publicly available material, they should be required to obtain a warrant or other form of authorisations to do so.

[315] Privacy Commissioner Michael Webster "Open Source Intelligence Conference Keynote Address 2022" (OSINZ Conference, 22 October 2022).

Targeted and non-targeted activity

6.46. As a broad proposition, when collecting information an Agency may be:

- focussing on a particular person or group they know or have reason to think may be involved in or has information about activities that, for example, threaten national security, which can be described, broadly, as targeted and reactive in nature
- attempting to discover any person or group who maybe a threat to national security, perhaps in response to concerning activities but with no particular person or group in mind, which is best described as non-targeted, discovery-type activity and proactive in character.

6.47. The discussion in chapter 5 about s 19 of the ISA is relevant to discovery work, and it is discussed further in chapter 8.

The relevance of nationality

6.48. As we noted in chapter 5, the ISA makes a distinction between New Zealand citizens and permanent residents (New Zealanders) and others (non-New Zealanders). There are tighter constraints around the purposes for which the Agencies can seek authorisations in relation to New Zealanders in four respects.

- First, warrants in respect of New Zealanders are referred to as Type 1 intelligence warrants and must be issued by the responsible Minister and a Commissioner of Intelligence Warrants whereas those in respect of non-New Zealanders are referred to as Type 2 intelligence warrants and may be issued by the Minister acting alone.
- Second, national security intelligence warrants can only be issued in respect of New Zealanders if the requirements of s 58(1)(a) are met. Specifically, the Minister and the Commissioner must be satisfied not only that the activity to be authorised under the warrant is necessary to contribute to the protection of national security but also that it "identifies, enables the assessment of or protects against" any of the certain specified harms.[316] This latter requirement does not apply in respect of non-New Zealanders.[317]
- Third, warrants to contribute to New Zealand's international relations or economic well-being can only be issued against New Zealanders where there are reasonable grounds to suspect that the relevant New Zealander may be acting on behalf of a foreign organisation or person or a designated terrorist organisation or is within a class of people employed by, or holding membership in, a foreign government or designated terrorist entity. By contrast, the responsible Minister may issue this type of warrant in respect of non-New Zealanders if satisfied that the warranted activity will contribute to New Zealand's international relations and well-being or to its economic well-being.
- Fourth, applications for permission to access 'restricted information'[318] are granted by both the relevant Minister and a Commissioner of Intelligence Warrants in the case of New Zealanders but only by the Minister in the case of non-New Zealanders. Access to New Zealanders' restricted information may only be granted if the access either:

[316] The requirement that the additional criteria set out in s 61 must also be met applies to New Zealanders and non-New Zealanders alike: see Intelligence and Security Act 2017, s 60(3)(c).

[317] Intelligence and Security Act 2017, s 60(3).

[318] As defined in the Intelligence and Security Act 2017, s 135.

- is necessary to the protection of national security *and* to assist in protecting against any of the harms listed in s 58(2); or
- will assist New Zealand's international relations and well-being or New Zealand's economic well-being **and** there are reasonable grounds to suspect that the relevant person is acting for a foreign organisation or person or a designated terrorist entity.

In relation to non-New Zealanders, however, access must simply be necessary to contribute to the protection of national security or to contribute to New Zealand's international relations and well-being or to New Zealand's economic well-being.[319]

6.49. While the ISA distinguishes between people based on their status as New Zealanders or non-New Zealanders, it does not distinguish based on where people are located. A Type 1 warrant may be issued in respect of a New Zealander wherever in the world that person may be, providing the relevant requirements are met. Similarly, a Type 2 warrant can be issued in respect of a non-New Zealander even though they happen to be in New Zealand at the time.

6.50. We return to the issue of nationality when considering the warranting framework in chapter 7 and restricted information in chapter 9.

Significance of retention and disposal provisions

6.51. As we noted in chapter 1, the broad way in which the principal objectives of the Agencies are stated means that there must be other mechanisms to control the scope of the Agencies' activities. Some of these mechanisms are institutional (such as the Inspector-General of Intelligence and Security and the Intelligence and Security Committee), while others take the form of statutory requirements or statutory limitations on powers.

6.52. The statutory provisions in relation to the retention and disposal of information after its collection and initial processing are an example of statutory provisions intended to control and limit the powers of the Agencies as part of the intelligence cycle outlined above.[320] Human rights considerations apply at all stages of this end-to-end process, and the balance between intelligence objectives and human rights interests such as privacy is struck both *within* stages in the cycle (for example when information is collected) and *between* stages in the cycle (for example, allowing the collection of more information for effective target discovery but having tighter restrictions on how such information may be used and when it must be destroyed). The operational effect of such provisions can offset the impact of broad powers of collection.

6.53. We discuss the retention and disposal of information under the ISA in chapter 8. We mention them now simply as a reminder that the Agencies' powers need to be viewed in a holistic way.

[319] In respect of both New Zealanders and non-New Zealanders, the additional requirements set out in s 139 must also be met.

[320] See chapter 8 for more discussion about the retention and disposal of information under the ISA.

CHAPTER 07
The warranting framework

Introduction

7.1. The warranting provisions of the Intelligence and Security Act 2017 (the ISA) provide the framework through which the intelligence and security agencies (the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) and referred to in our report as 'the Agencies') are authorised to carry out activities that would otherwise be unlawful.[321] Because a warrant allows the Agencies to undertake otherwise unlawful acts, the grant of a warrant gives rise to a greater likelihood that the actions it enables will impinge on personal freedoms, such as privacy.

7.2. As described in chapter 6, the process for obtaining warrants, and the criteria that have to be met, differ as between New Zealanders (ie, citizens and permanent residents) and non-New Zealanders. In terms of obtaining warrants against New Zealanders, the process is more complex, in that a Commissioner of Intelligence Warrants must issue warrants jointly with the responsible Minister. In terms of the relevant criteria, the requirements in respect of New Zealanders are more onerous than in the case of non-New Zealanders.[322] These differences are clearest in the Type 1 / Type 2 warrant distinction.

7.3. In the debates during the passage of the ISA through Parliament, members referred to the scheme for warrants in respect of New Zealanders (ie, Type 1 warrants) as a 'triple lock' scheme – that is, it requires decisions by both the Minister and a Commissioner of Intelligence Warrants that a warrant should be issued, as well as a subsequent review by the Inspector-General of Intelligence and Security (Inspector-General).[323] The use of the term 'triple lock' suggests that members expected each element of the process to be meaningful.

7.4. The issuing of warrants and the carrying out of warranted activities are explicitly subject to oversight by the Inspector-General, whose office receives and reviews all warrants obtained by the Agencies. The Inspector-General has consequently issued two specific reports dealing with warranting under the ISA.[324]

---

[321] Intelligence and Security Act 2017, s 49.

[322] The requirements are only slightly more onerous in the case of warrants for the protection of national security, but significantly more onerous in the case of warrants for international relations or economic well-being.

[323] See, for example, (18 August 2016) 716 NZPD (New Zealand Intelligence and Security Bill – First Reading speech of Hon Christopher Finlayson KC).

[324] Inspector-General of Intelligence and Security *Report on warrants issued in the first months of the Intelligence and Security Act 2017* (December 2018) and *Inspector-General of Intelligence and Security Warrants issued under the Intelligence and Security Act 2017 update* (November 2019).

7.5. To be effective, the process for the grant of warrants needs to be rigorous. There is also a need for candour on the part of the Agencies because they are made *ex parte* (without notice). Additionally, unlike warrants obtained by the Police, the grant of warrants to the Agencies is unlikely to be the subject of scrutiny by the courts. While warrants are reviewed by the Inspector-General, there is little prospect of there being a judicial review challenge in court and, therefore, a contest of views on whether a warrant should be granted. We return to this later in our discussion.

Principles applicable to a warranting framework

7.6. In this chapter, we recommend amendments to the warranting provisions of the ISA. The terms of reference require us to consider "whether the authorisation framework under the Act can be improved to better serve the purpose of the ISA".[325] Our suggested amendments are based on several principles that have provided a framework for our review. These principles are:

- the purpose of intelligence is to protect New Zealand as a free, open and democratic society, underpinned by the rule of law[326]
- human rights should be recognised and respected
- social licence requires that there be as much transparency as possible in the way that the Agencies operate
- the warranting framework should be certain and able to be implemented effectively
- the warranting framework needs to be technology neutral, even as available technologies change and evolve.

7.7. Our recommended amendments should not be taken as a criticism of the Agencies. Based on our observation, there is a reasonably strong culture within the Agencies that focuses on compliance with the obligations and processes set out in the ISA. Despite this observation, we consider that the ISA should be more explicit in describing the obligations and information requirements placed on the Agencies when seeking warrants. This serves several purposes: first, it should assist the Agencies by providing certainty over what is required when applying for a warrant; second, it will assist those charged with control and oversight of warranting; third, it will give the public greater insight, and therefore comfort, about the approach being taken to the issue of warrants under the ISA.

Issues arising during our review

7.8. There are several issues that have arisen in relation to the warranting framework that we have considered during our review. Some of these issues have been discussed elsewhere in this report (such as lawfulness and whether warrants should be required for hacked and leaked datasets that are 'open-source' because they have been published on the internet). This chapter first provides an overview of the warranting framework and then deals with the following questions.

- Should the distinction between Type 1 and Type 2 warrants be retained?
- If not, should the ISA continue to differentiate between New Zealanders and non-New Zealanders?

[325] Appendix A.
[326] Appendix A.

- Should the duty of candour be expressly mentioned in the ISA?
- Is the information that the ISA requires to be provided in warrant applications sufficient?
- What approach should be taken to warrants for classes of persons?
- Is the warranting regime sufficient to keep pace with technological and analytical advances to effectively address target discovery?
- Is the approach to necessity and proportionality appropriate?

7.9. We conclude by proposing an alternative warranting scheme.

Overview of the warranting framework

7.10. Warranting is provided for in the authorisation regime in Part 4 of the ISA. The authorisation regime includes two types of intelligence warrants mentioned earlier, as well as provisions for urgent intelligence warrants, very urgent authorisations, and removal and practice warrants. Our focus in this review has been on the intelligence warrants. We propose no changes to the other types of warrants.[327]

7.11. Type 1 warrants may be issued in respect of New Zealanders for two broad purposes.

- To enable an Agency to carry out an activity that (i) is necessary to contribute to the protection of national security and (ii) identifies, enables the assessment of, or protects against, certain specified harms.[328]
- To enable an Agency to carry out an activity that will contribute to either the international relations and well-being of New Zealand, or the economic well-being of New Zealand, where there are reasonable grounds to suspect that:
  - the relevant New Zealander is acting for or on behalf of a foreign person or organisation or a designated terrorist entity
  - the person is a member of a class of non-New Zealanders against whom an Agency proposes to take action and is employed by or is a member of a foreign government or a designated terrorist entity.[329]

  This notion is sometimes referred to by way of shorthand as "an agent of a foreign power".[330]

[327] Any removal of the Type 1 / Type 2 distinction will, of course, require consequential changes to the provisions of the ISA on urgent intelligence warrants and very urgent authorisations.

[328] Intelligence and Security Act 2017, s 58.

[329] Section 59.

[330] This phrase was not specifically used in the Government Communications Security Bureau Act 2003, although the definition of "foreign organisation" in s 4 of the Act included "a person acting in his or her capacity as an agent or a representative of any Government, body, or organisation". The concept was the subject of discussion in the Cullen/Reddy report: Hon Sir Michael Cullen, KNZM, and Dame Patsy Reddy, DNZM, *Intelligence and Security in a free Society – Report of the First Independent Review of Intelligence and Security in New Zealand* (29 February 2016) at [5.73]-[5.77] and [6.77]. The phrase is not used in the ISA.

7.12. Type 2 warrants may similarly be issued to enable an Agency to carry out an activity that is necessary to contribute to the protection of national security or will contribute to the international relations and well-being of New Zealand, or the economic well-being of New Zealand.[331] A Type 2 warrant may not authorise an activity for which a Type 1 warrant is required.[332]

7.13. Currently, the process by which a warrant may be granted depends on whether the warrant being sought is a Type 1 or Type 2 warrant. Type 1 warrants must be issued by the Minister and a Commissioner of Intelligence Warrants. This means that both the Minister and the Commissioner must be satisfied that the requirements of the ISA have been met and that it is appropriate for the warrant to be issued. Type 2 warrants need only be issued by the Minister.

7.14. All intelligence warrants must comply with additional criteria set out in s 61 of the ISA. These include that: [333]

- the proposed activity is necessary to enable the Agency to perform a function under s 10 or s 11
- the proposed activity is proportionate to the purpose for which it is to be carried out
- the purpose of the warrant "cannot reasonably be achieved by a less intrusive means".

7.15. A warrant may authorise a wide variety of otherwise unlawful activities, such as surveillance, interception and/or seizure of communications and other items, searches, human intelligence activity and requests to foreign governments or other entities to do things that a New Zealand agency would require a warrant to do.[334] The Director-General of the relevant Agency (or an authorised employee) may exercise a variety of powers to give effect to a warrant, including doing "any other act that is reasonable in the circumstances and reasonably required to achieve the purposes for which the warrant was issued".[335] This is, however, subject to any restrictions or conditions in the warrant itself.[336] The Director-General may also request assistance with giving effect to a warrant from the Police or any other organisation or person.[337]

7.16. To the extent that warrants are being issued for purposes associated with the protection of national security, we consider it is an issue that the ISA does not include a definition of 'national security'. In the absence of this, the concept of national security is largely guided by the National Security and Intelligence Priorities (NSIPs).[338] In the case of New Zealanders, s 58 contains criteria that must be met before national security warrants can be issued. As noted in chapter 5, these criteria have the effect of narrowing the scope of 'national security' as it applies to New Zealanders, although it is still broad. However, that limitation does not apply in the case of non-New Zealanders, which means that there is an even broader range of matters that could be justified as being for the purposes of national security.

---

331 Intelligence and Security Act 2017, s 60. As noted below, s 61 requires that all warrants must meet additional criteria, including that the proposed activity by an Agency is necessary to enable the Agency to perform a function under s 10 or s 11 of the ISA.

332 Section 60(3)(b).

333 Section s 61(a), (b), and (c). Section 61(d) also requires that satisfactory arrangements are in place to ensure that nothing is done beyond what is necessary and proportionate to perform a function, steps are taken to minimise impacts on members of the public and any information obtained is only retained, used and disclosed in accordance with the law.

334 Section 67.

335 Section 68(1) (NZSIS) and s 69(1) (GCSB).

336 Section 68(2) and s 69(2).

337 Section 51.

338 Section 10(1) makes it a function of the Agencies to collect and analyse in accordance with the government's priorities. The NSIPs are the key mechanism for the government to set out its priorities.

7.17. As discussed earlier in this report,[339] we recommend that a definition of 'protection of national security' be included in the ISA.[340] Our proposed definition is threats-based and would remove the need for s 58(1)(a)(ii) and the list of harms referred to in s 58(2). It will also have other consequences, which we will discuss later in this chapter.

7.18. If that recommendation is accepted, all threats-based warrants should, as a matter of principle, be sought as warrants to contribute to the protection of national security; non-threats-based warrants would be sought as warrants to contribute to international relations or well-being, or economic well-being.[341] We return to the reporting of the purpose of intelligence warrants in the following section.

Intelligence warrants

7.19. As discussed above, the ISA provides a framework for intelligence warrants based on the Type 1 / Type 2 distinction. The Agencies are required to state in their annual reports the number of applications they have made for Type 1 and Type 2 warrants, the number granted and the number declined.[342] However, this framework obscures the nature and purpose of warranted activities, which are varied and have different impacts on privacy and other human rights, from little or low impact to high impact. We consider that the ISA should require the Agencies to report in a way that is more meaningful and therefore transparent for the New Zealand public.[343]

7.20. We consider that greater transparency will be provided if the Agencies are required to report against the principal objective and the function to which warrants relate. To explain, s 9 sets out the three principal objectives of the Agencies as contributing to:

- the protection of New Zealand's national security
- New Zealand's international relations and well-being
- New Zealand's economic well-being.

7.21. The warranting provisions mirror these objectives in that they enable the Agencies to obtain warrants for each objective. Sections 10, 11 and 12 set out the relevant functions of the Agencies, namely:

- collecting and analysing intelligence in accordance with the government's priorities (s 10)
- providing protective security services, advice and assistance to public authorities and others (s 11)

---

339 See chapter 5.

340 The proposed definition is: "**protection of national security** means the protection of New Zealand, its communities and people from activities that are threats because they undermine, or seek to undermine, one or more of New Zealand's territorial integrity and safety, including the safety of its communities and people; sovereignty, democratic institutions, processes and values; multi-cultural and diverse social fabric; and essential interests, including its critical infrastructure and governmental operations; and includes identifying and enabling the assessment of such threats", with the possible addition of wording such as "Such activities include, but are not limited to, terrorism, espionage, sabotage, violent extremism, insurrection, foreign interference, cyberthreats and serious transnational crime".

341 There may also be warrants that authorise otherwise unlawful information assurance and cybersecurity activities, which are addressed in the following section.

342 Intelligence and Security Act 2017, s 221(2).

343 Of course, if the distinction between Type 1 and Type 2 warrants is abolished, as we recommend in the next section, an alternative form of reporting will have to be found in any event.

- in relation to GCSB, providing information assurance and cybersecurity activities to public authorities or others and doing everything necessary or desirable to protect the security and integrity of important communications and information infrastructures, including identifying and responding to threats or potential threats to them (ss 11 and 12).

7.22. We consider that the Agencies' reporting requirements in relation to warrants should be framed in terms of both the s 9 objective and the ISA function to which warrants relate. This should not be a burden for the Agencies as a warrant must state what type of warrant it is, the objective in s 9 to which it relates and its purpose.[344] We would add one further category for reporting, namely dataset acquisition, which we deal with in the target discovery section below.

7.23. Reporting on this basis will provide further information (albeit still very general information) about the areas in which the Agencies are focusing their work. This may assist both the members of the Intelligence and Security Committee in the performance of their oversight functions in relation to the Agencies and the public's understanding of what the Agencies do, which may assist with enhancing the social licence of the Agencies.

Treating New Zealanders and non-New Zealanders differently

7.24. As we noted in chapter 6, a key feature of the warranting regime is the different treatment of New Zealanders and non-New Zealanders. The question as to whether, and if so to what extent, the nationals of a country might be treated differently to non-nationals arises most prominently in the context of the surveillance activities of security and intelligence agencies and the impact of those activities on the right to privacy. The question is complex. Not surprisingly, no single perspective exists on whether it is appropriate to differentiate between nationals and non-nationals. Those who favour differential treatment focus on, amongst other things, the specific obligation owed by a state to its own citizens and the importance of safeguards to ensure a free press and the opportunity for political dissent within a democracy.[345] Those who favour the same treatment for nationals and non-nationals emphasise the universality of human rights, including in particular, the right to privacy. They also point out that technological developments, with the resulting impact on how we communicate and store information, make distinctions based on nationality a lot less meaningful.

7.25. In the context of the ISA, the review carried out by Sir Michael Cullen and Dame Patsy Reddy (Cullen/Reddy review) proposed retaining the distinction between New Zealanders and non-New Zealanders (which was made in the 2003 GCSB Act), saying:[346]

> The government, as part of its role in protecting national security, has an obligation to protect the rights of its citizens and permanent residents. We consider this is appropriately achieved by applying a higher threshold for authorising activities directed at New Zealanders than in respect of foreign citizens, whose own states are responsible for protecting their rights.

---

344 Intelligence and Security Act 2017, s 66.

345 See for example Peter Swire, Jesse Woo, and Devan R Desai *The Important, Justifiable and Constrained Role of Nationality in Foreign Intelligence Surveillance* Aegis Series Paper No. 1901, 10 January 2019.

346 Hon Sir Michael Cullen, KNZM, and Dame Patsy Reddy, DNZM, *Intelligence and Security in a free Society – Report of the First Independent Review of Intelligence and Security in New Zealand* (29 February 2016) at [5.61] (*Cullen/Reddy report*).

7.26. The Cullen/Reddy report also considered that it would not be appropriate for New Zealanders to be the subject of the Agencies' intrusive powers for the broader purposes of advancing New Zealand's economic and international interests, as this would be inconsistent with New Zealand's status as a free and democratic country and would entail an unjustifiable intrusion on New Zealanders' privacy and liberty, although they did recognise the possibility of a limited exception.[347]

7.27. As part of our public engagement process, we asked whether it is important for New Zealanders to have more protections compared with non-New Zealanders when the Agencies collect information to identify and assess national security risks. A number of submitters remained in favour of greater protections for New Zealanders over non-New Zealanders citing the state's duty to protect the rights of citizens and to protect citizens against threats. However, the majority of respondents did not consider it important that New Zealanders have more protections compared with non-New Zealanders when the Agencies are collecting information. These respondents saw national security threats as coming from both overseas and domestic sources and believed that both sources of threat should be treated equally. They also considered that human rights and the right to privacy are universal, regardless of national origin.

7.28. Within the Five Eyes partnership, the United Kingdom draws no distinction between citizens and non-citizens.[348] This is consistent with the United Kingdom's obligations under the European Convention on Human Rights, in which human rights for those within a state party's jurisdiction may not be discriminatory on the basis of citizenship or nationality.

7.29. The remaining Five Eyes partners continue to distinguish between nationals and foreigners and have not shown any desire to alter this position. For example, the 2019 Review of the Australian National Intelligence Community by Dennis Richardson noted that:[349]

> All liberal democratic countries have different processes – either in law or in practice – for the targeting of their own citizens, recognising the higher political risks for governments engaging with their own people.

7.30. Human rights organisations have, not surprisingly, supported the United Kingdom approach, arguing that all persons are entitled to non-discriminatory treatment and equal protection of the law and that therefore no distinction should be drawn in intelligence collection activities between citizens and non-citizens.[350] This is based on the non-discrimination provisions of the International Covenant on Civil and Political Rights (ICCPR).

---

347 Above n at [5.64]. The possible exception was where a New Zealander was an agent of a foreign power: see [5.77]. Section 59 gives effect to this exception.

348 See the Investigatory Powers Act 2016.

349 Dennis Richardson *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community* Australian Attorney-General's Department, December 2019, Volume 1 at [3.36].

350 Electronic Frontier Foundation, *Necessary and Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance: Background and Supporting International Legal Analysis* (May 2014) at 4-7. The New Zealand Human Rights Commission/Te Kāhui Tika Tangata also supported this comprehensive approach in its submission to us.

Should the Type 1 / Type 2 distinction be retained?

7.31. Despite the view expressed in the Cullen/Reddy report and the position taken by the majority of the Five Eyes countries, we do not consider that the distinction between Type 1 and Type 2 warrants remains meaningful. This view is consistent with what we heard from many of those we consulted with who are familiar with the warranting framework, including the Agencies.[351] Additionally, the Inspector-General did not oppose the removal of the distinction. As we will explain, the Agencies commonly obtain 'partner' warrants – Type 1 and Type 2 warrants together – which means that the distinction is effectively meaningless. It creates unnecessary work for the Agencies and for those who issue warrants for no purpose. We therefore do not believe there is merit in retaining this distinction.

7.32. Rather, we consider that:

- All intelligence warrants should be issued by both the responsible Minister and a Commissioner of Intelligence Warrants. Accordingly, both New Zealanders and non-New Zealanders would have the benefit of the 'triple lock'
- Warrants for the protection of national security would be issued against New Zealanders and non-New Zealanders on the basis of the same criteria, ie, on the basis of the proposed definition of 'protection of national security' (if it is accepted) and the other relevant criteria (such as necessity and proportionality)
- In respect of warrants for international relations or economic well-being there are three options:
  - they would not be available against New Zealanders
  - they would be available against New Zealanders but only on the basis of the additional criteria that currently apply[352]
  - they would be available against New Zealanders on the same basis as they are available against non-New Zealanders.

7.33. While we do not have a strong view about it, our inclination is to favour the second of the three options, which is generally in line with the present position. It is also consistent with the Cullen/Reddy report as noted in paragraph [7.25] above. This can be implemented by setting out the relevant criteria in a single section, without the need to maintain the Type 1 / Type 2 distinction. Given the nature of these warrants (to contribute to New Zealand's international relations and well-being or economic well-being), we do not see a distinction between New Zealanders and non-New Zealanders as unjustifiably discriminatory.

7.34. We now explain our views.

7.35. We acknowledge that the government owes specific obligations to its own citizens and permanent residents (ie, to New Zealanders). However, New Zealanders will not be worse off if the distinction between Type 1 and Type 2 warrants is removed:

---

[351] The Royal Commission of Inquiry also stated that "Given the practical difficulties that the distinction causes, it may be more straightforward to provide for a single category of warrant, at least for counter-terrorism". Royal Commission of Inquiry *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020), part 8, chapter 14, at [105] (*Royal Commission report*).

[352] The current s 59 criteria only allow targeting of a New Zealander for international relations or economic well-being purposes if the New Zealander is acting for foreign organisations such as governments or designated terrorist entities.

- In relation to warrants for the protection of national security, all that would happen is that non-New Zealanders would have the same level of protection as New Zealanders from a human rights perspective. This would not be a bad outcome. In fact, from a human rights point of view, this would be the better approach. It would not diminish the level of protection available to New Zealanders.
- In relation to warrants for international relations or economic well-being, the differential criteria in s 59 could be retained so that the additional protection for New Zealanders would remain, but without retaining the Type 1 / Type 2 distinction. (This, of course, assumes that the second of the three options in paragraph [7.32] is adopted.) This would alter the form of authorisation, but not enlarge the scope for targeting New Zealanders. Like warrants for the protection of national security, all warrants for international relations or economic well-being would be issued by both the Minister and a Commissioner of Intelligence Warrants.

7.36. Removing the Type 1 / Type 2 warrant distinction would also be consistent with the Agencies' existing practice. In 2019, the Acting Inspector-General expressed the view that Type 1 and Type 2 warrants should be obtained together when collateral or incidental collection of New Zealanders' communications is expected in the course of foreign intelligence activities under a Type 2 warrant.[353] The Acting Inspector-General noted that there was a difference of view between her office and the Solicitor-General about when a Type 1 warrant was required in these circumstances:[354]

- The Agencies' and the Solicitor-General's view was that a Type 1 warrant was not required by s 53 of the ISA where the Agency had no intention to collect the communications of New Zealanders even if such collection was a possible or likely effect of intercepting the communications of non-New Zealanders under a Type 2 warrant. The need to obtain a Type 1 warrant would only arise if the Agency wished to utilise a New Zealander's incidentally collected information for intelligence purposes about the New Zealander. In short, the subjective intent of the Agency was the determinative factor.
- The Inspector-General's view was that given the privacy interests involved, a Type 1 warrant should be obtained where it was "reasonably expected" that an Agency would collect New Zealanders' information in the course of foreign intelligence activities under a Type 2 warrant. In her view, the critical aspect was not the Agency's subjective intent but the likely effects of the warrant on New Zealanders' privacy interests.

7.37. This is not a debate we will dwell on, other than to say we prefer the Inspector-General's view, although we acknowledge that the Agencies are required to follow advice of the Solicitor-General.[355] We mention the issue because it shows some of the difficulties that have arisen from the Type 1 / Type 2 distinction. The result is that the Agencies commonly obtain 'partner' warrants – Type 1 and Type 2 warrants together. This means that the distinction between Type 1 and Type 2 warrants has little, if any, practical effect. All the distinction does is impose a greater administrative burden on the Agencies, but to no real end. In submissions to the review, both Agencies said that they support the removal of the distinction, and the Inspector-General queried whether the distinction continued to serve a useful purpose.

---

353 Inspector-General of Intelligence and Security *Warrants issued under the Intelligence and Security Act 2017 - 2019 update* (November 2019) at [22].

354 Above n, at [21]–[22].

355 As noted in the Inspector-General's report (at 4 footnote 6), the Inspector-General did not ask the Agencies to seek waiver of legal privilege in relation to the Solicitor-General's advice and – as here – the content of the advice was not discussed. For the purpose of our review, we have assumed that the Inspector-General accurately recorded the Solicitor-General's view.

Warrant applications and the duty of candour

7.38. In the past, the Inspector-General has been critical of the approach taken by the Agencies when making warrant applications. This led the Inspector-General to recommend that additional detail be provided in warrant applications so that the decision makers have a good idea of what is to be covered by the warrant.[356] According to the Inspector-General, the Agencies have since improved both the level of detail provided in warrant applications and their conciseness.[357] Despite the Agencies having made changes, we consider that the ISA should provide greater clarity as to the level of detail the Agencies should provide when seeking a warrant. This will give greater certainty to the Agencies as to the information they must provide when seeking a warrant and a clearer standard for the Minister and Commissioners to apply when considering warrant applications. It will also provide further transparency to the public about the matters that inform warranting decisions.

7.39. As it stands, the ISA provides only general guidance as to what the Agencies should provide when seeking a warrant. This is set out in s 55 of the ISA, which requires the Agencies to provide:

- the type of intelligence warrant applied for
- details of the activity proposed to be carried out under the warrant
- the grounds on which the application is made (including the reasons why the legal requirements for issuing the warrant are believed to be satisfied)
- a statement in which the Director-General making the application confirms that all of the information set out in the application is true and correct.

7.40. In addition to the matters set out in s 55, the Agencies accept they have a general obligation of candour applying at common law when seeking warrants.[358] The Inspector-General has described this obligation as being to "ensure comprehensive disclosure of material information; to address the specific requirements of the empowering legislation; and to ensure that actions are directed principally at the [Agencies] own statutory purposes".[359]

7.41. The Court of Appeal has emphasised the importance of the duty of candour in the context of Police and other public agencies seeking search warrants. We mention two of these authorities. The first is *Tranz Rail Ltd v Wellington District Court*.[360] In that case, the Commerce Commission obtained a search warrant under the Commerce Act 1986 against Tranz Rail to ascertain whether Tranz Rail had engaged in conduct that breached ss 27 or 36 of the Commerce Act. Tranz Rail challenged the grant of the warrant. In the course of its judgment upholding Tranz Rail's challenge, the court made three important points:

---

356 Inspector-General of Intelligence and Security *Warrants issued under the Intelligence and Security Act 2017* (December 2018) at [84–98].

357 Inspector-General of Intelligence and Security *Annual Report for the year 1 July 2020 to 30 June 2021* (online, 11 November 2021) at 16.

358 Both Canadian and United Kingdom authorities have acknowledged the duty of candour owed to warrant issuers by intelligence and security agencies: see Government of Canada *Policy of the Department of Justice Canada and the Canadian Security Intelligence Service on the Duty of Candour in* ex parte *Proceedings* (2 December 2021); Investigatory Powers Commissioner's Office *Approval of Warrants, Authorisations and Notices by Judicial Commissioners* (Advisory Notice 1/2018, 8 March 2018).

359 Inspector-General of Intelligence and Security *Inquiry into New Zealand Security Intelligence Service applications for sensitive and complex warrants* (online, November 2016) at [7].

360 *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA).

- First, applications for search warrants are almost always made without notice to the person affected.
- Second, given the 'without notice' nature of a warrant application, the judicial officer asked to issue the warrant is entitled to expect the applicant to make "full and candid disclosure of all facts and circumstances relevant to the question whether the warrant should be issued".[361] In short, the judicial officer must be given the 'full picture'.
- Third, given the need to present the full picture, a warrant application should refer to everything known to the applicant that "might be relied on by the target of the warrant if that person had the opportunity to appear in opposition."[362]

7.42. The second case is *R v Williams*,[363] which concerned a search warrant issued under s 198 of the Summary Proceedings Act 1957. There, all members of the court reiterated the importance of a judicial officer who is asked to issue a warrant being given **all** relevant information in the warrant application.[364]

7.43. While applications for intelligence warrants are not directly analogous to applications for search warrants, we see the duty of candour being even more important in relation to the Agencies. Obviously, applications for intelligence warrants are made on a 'without notice' basis. They do not come within the purview of a court (much less an open court) that could examine the basis on which they were granted. In respect of Type 1 warrants, the Commissioners of Intelligence Warrants (retired High Court judges) have a judicial function to perform. They are entitled to expect that they will be provided with all relevant information on the issues they are asked to consider before granting a warrant. This includes any information known to the relevant Agency that undermines the case for a warrant.[365]

7.44. In addition, if there are legal issues of which the Agency is aware in relation to the granting of the warrant, they should be brought to the attention of the Commissioners, explicitly and obviously. As the English Court of Appeal put it in an analogous context, the process must be conducted "with all cards face upwards on the table".[366]

7.45. Given the importance of the duty of candour, and the fact that it is already acknowledged by the Agencies, we believe specific reference should be made to it in the ISA. This would be done by adding a reference to the duty of candour in s 17 of the ISA alongside the other general duties of the Agencies. Section 17 is an appropriate place for referring to the duty of candour because the application of the duty will not just be limited to warrant applications.[367]

7.46. We think it important that the ISA state the duty explicitly for the following reason. In the criminal context, where the duty of candour also applies, it is unnecessary to spell the duty out in legislation because it is an issue that can be addressed by the courts when required. Warrants in a law enforcement context are often examined in subsequent criminal proceedings for procedural

---

[361] Above n, at [21].

[362] Above n, at [22].

[363] *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207.

[364] See Glazebrook J (with whom Young P agreed) at [214] and Hammond J at [268]-[270].

[365] We note that Advisory Notice 1/2018 issued by the UK Investigatory Powers Commissioner's Office discusses the duty of disclosure applying to applicants for warrants in terms consistent with the discussion in the text: see [30]–[35]. The UK system is different in that the Judicial Commissioners decide whether to approve decisions made by the Secretary of State to issue warrants, but the principles are similar.

[366] *R v Lancashire County Council, ex parte Huddleston* [1986] 2 All ER 941 (CA) at 945.

[367] For example, it will also be relevant to applications for permission to access restricted information under s 136 of the ISA.

shortcomings. When defence counsel challenges the basis on which a warrant was issued, the courts must adjudicate the issue. In that context, the courts have an opportunity to reaffirm and reinforce – publicly – fundamental principles such as the duty of candour. Accordingly, the criminal process, which is adversarial and fundamentally open, provides a setting in which the duty of candour and similar matters can be addressed other than by being dealt with in legislation.

7.47. The same is not true in relation to the Agencies operating in an intelligence and security setting. Issues relating to intelligence warrants are unlikely ever to be adjudicated by the courts. The Minister and Commissioners are unlikely to be aware of any departure from the duty in a particular case. It is possible that the Inspector-General could become aware of a failure to adhere to the duty in a particular instance and identify it as an irregularity, but that would be difficult. Setting the duty out in the ISA as a fundamental principle to which the Agencies must adhere in seeking authorisations serves a similar purpose to that served by the courts when they address such issues – it states **publicly** a fundamental standard with which the Agencies are expected to comply.

7.48. We also do not think that the application of the duty of candour should be limited to the warranting provisions in Part 4 of the ISA, although we do note in our recommendation that the Agencies should be required to comply with the duty while performing **relevant** functions. We have two reasons for expressing our recommendation in this way. First, to the extent that the duty of candour currently applies as a matter of common law, it applies generally. Our intention is that the duty be made explicit in the ISA. It is not to limit the extent to which the duty currently applies, and there is a real risk of this occurring if the duty is said to only apply to Part 4 of the ISA. Second, it is clear the duty of candour applies beyond Part 4. It would also apply, for example, to applications for approval to access restricted information under Part 5 dealings with the Inspector-General and the Intelligence and Security Committee under Part 6 and engaging with the periodic reviews of the ISA under Part 7. In saying this, we accept that there are matters to which the duty would not apply, such as dealings with the public or where there are express restrictions on the disclosure of information. This is why we have recommended that the duty should apply where relevant.

7.49. Alongside referring to the duty of candour, we believe that s 55 should be amended so that the categories of information required in a warrant application are specified in more detail.[368] Besides being required to identify any issues or potential weaknesses in the warrant application, the Agencies should also be required to detail the information relevant to the necessity and proportionality assessment, the likelihood of third-party information being collected and the approach that will be taken to data retention, storage and destruction. We also consider that if the application is for a renewal or a repeat warrant, the application should specifically address why the authorisation should be continued and the value of the information obtained under the previous warrant(s).

7.50. The full list of the information requirements we recommend be included in an updated section 55 is set out in the recommendations section at the end of this chapter.

[368] We acknowledge that information should be provided in order to meet the requirements in s 61 that satisfactory arrangements are in place covering certain matters. We consider that the explicit recognition of these information requirements in s 55 would assist in public awareness of the precise nature of information required to be in an application.

Warrants targeting a class

7.51. The ISA does not set the level of specificity required for warrants identifying a target class and determining whether a specific individual falls within that class. The Royal Commission report observed that the level of detail has been the subject of attention by the Inspector-General.[369] This applies particularly to the GCSB, which tends to seek authorisations to target relatively wide classes of persons, whereas the NZSIS has tended to seek warrants in respect of particular individuals or groups of individuals. Although the Agencies take different approaches to the collection of intelligence against a target class of persons, the purposes of the collection are generally the same: ie, to identify persons within a class who are of security or intelligence interest or to collect intelligence from and about these people. Some class warrants with a discovery purpose may be relatively broad. As a result, information will be obtained about people who are not of intelligence interest. For those who are of intelligence interest, collection may continue either under an existing class warrant or when a new authorisation is sought.

7.52. There are four issues that arise from class warrants:

- the identification of the class that should be the subject of the warrant, including the threshold for determining whether a person fits within a class
- the lack of statutory guidance on when individual or class warrants should be sought
- assessing whether the class warrant is necessary and proportionate
- how the information obtained about individuals who are not of intelligence interest should be treated.

7.53. The discussion below deals with the first two issues. The remaining issues are dealt with later in this chapter (in the case of necessity and proportionality) and in chapter 8 (the treatment of information about individuals that are not of intelligence interest).

7.54. The specificity in the identification of the class of persons that should be the subject of a warrant has been identified as an issue by the Inspector-General in the past, with respect to GCSB.[370] This appears to have been largely resolved by GCSB seeking to define the class with as much specificity as possible for the authorisation to ensure that there is certainty over who falls within it. This should continue, as should the provision of information on the particular characteristics that the persons in the class share or the common activities in which they are involved. It is also the practice of the Agencies to set out the process for confirming an individual falls within the scope of the class in the warrant application, including the criteria to be used for determining if an individual fits in a target class, the process for undertaking the proposed activities against an individual and the application of the necessity and proportionality tests. Our recommendations support these practices continuing.

7.55. This gives rise to the second issue, which is that the ISA gives no guidance on when it is appropriate to use a process for determining whether an individual fits within a broad class warrant instead of a specific individual warrant. In principle, the use of highly intrusive covert surveillance activities against any individual, who may be of national security concern, should be authorised by way of an individual warrant. This provides the issuers with the opportunity to consider the particular circumstances of the individual concerned and gives them an opportunity to impose additional restrictions or conditions on the warrant, specific to the individual, should

[369] For examples, see Royal Commission report part 4, chapter 14, at [92]-[99] and part 8, chapter 14 at [95].

[370] Inspector-General of Intelligence and Security *Warrants issued under the Intelligence and Security Act 2017* (online, December 2018) at 23.

they wish to do so. Establishing a process within the warrant for determining whether a person fits within a class warrant, even if there is reporting to the warrant issuers of the number of persons that are part of the class, does not allow the issuers the opportunity to assess the necessity and proportionality of the proposed activities against a specified individual or individuals. Instead, with class warrants the Agencies are effectively given the discretion to decide whether an individual should be included within a class without having to go through the external checks that accompany the warranting process.

7.56. The Inspector-General raised this as an issue at the late stages of our review. We have therefore not been able to properly consider the issue. However, it is a potentially significant issue. We acknowledge the importance of class warrants, especially in the context of discovery activities and when dealing with groups, such as terrorist groups or state actors. The difficulty is that it cannot be assumed that all members of a class are the same and should be dealt with in the same way without further issuer oversight. This is therefore a matter that requires further, and more detailed, consideration.

7.57. As a final matter, we have considered the retention of class warrants and whether the introduction of 'purpose-based warrants' may be more appropriate, as recommended by the Cullen/Reddy report. A clause to this effect was deleted from the New Zealand Intelligence and Security Bill at select committee stage because it was considered that Type 1 and Type 2 class warrants could meet the operational needs of the Agencies, which purpose warrants were meant to serve.[371] Although we have recommended the removal of the Type 1 / Type 2 distinction, we do not consider there is a need to move to purpose-based warrants. Instead, we consider that the issues raised by class-based warrants can be addressed through the amendments we are recommending in relation to providing more detail on how a class should be defined and the process for determining whether persons fit within a class, assessing whether the warrant is necessary and proportionate and the rules relating to the retention, use and disposal of information.

Target discovery

7.58. The terms of reference state that the review will have particular regard to whether the ISA sufficiently enables and controls target discovery activity by the Agencies. Chapter 4 has already examined this issue from the perspective of s 19 of the ISA. This section examines target discovery in relation to the collection and acquisition of bulk datasets.

7.59. The Royal Commission discussed target discovery, which it described as "a proactive, exploratory effort to generate and investigate leads" to help identify "previously unknown, specific subjects of interest".[372] In the context of the Royal Commission, the focus was on a previously unknown 'lone actor'. Outside that context, however, target discovery is broader than identifying individuals. It includes gaining insights and better understanding of actors and trends in security interests. The Royal Commission noted the importance of analysing data and information, both already collected as well as intelligence gathering online, including through the collection of large datasets.[373]

7.60. As was noted in chapter 6, intelligence and security agencies may download hacked and leaked datasets from the internet, may use technological tools to scrape the internet for data and

[371] Foreign Affairs, Defence and Trade Committee *New Zealand Intelligence and Security Bill (158-2)* (24 February 2017) at 6.
[372] Royal Commission report, part 8, chapter 10 at [4].
[373] Royal Commission report, part 8, chapter 10 at [5].

may aggregate information from different sources for intelligence purposes, including to identify persons of security interest. The Royal Commission referred to the debate over the appropriateness of intelligence and security agencies obtaining large quantities of what it referred to as 'bulk data'.[374] As the Royal Commission said, the key feature of bulk data collection is that "a large proportion of the data gathered relates to people who are not intelligence targets and is of no intelligence value".[375]

7.61. There is no clear demarcation between bulk collection and targeted collection under a class warrant with a broadly defined class; rather, there is a 'continuum' with bulk collection at one end and a closely defined class warrant at the other.[376] Nevertheless, we see a material difference between the usual warranted activities of the Agencies targeted at people within a target class under a class warrant and the acquisition of bulk datasets for target discovery purposes.

7.62. Where intelligence and security agencies have access to bulk datasets, they use selectors, cross-referencing and other analytical tools to filter out what is relevant for their functions, with the objective of making linkages and discovering anomalies or unknowns that are of national security interest. In line with this objective, the NZSIS is seeking to improve its ability to discover, connect and use information through its Discover Strategy.[377] The Inspector-General has started a review of the NZSIS's target discovery activities and has scheduled a review of both Agencies' acquisition and use of bulk personal datasets.[378]

7.63. On the face of it, the ISA enables the acquisition, use and retention of bulk personal datasets, provided the necessity and proportionality tests can be met. However, from what we have heard from those familiar with the warrant issuing process, this can itself be a challenging endeavour as 'necessity' in the context of target discovery raises a circular issue. Without knowing whether anything of intelligence value will be identified, it becomes difficult to assess necessity and proportionality at the warrant issuing stage for some discovery activities as the value of the activity can only be ascertained once it has occurred. As one consultee put it, "you know you're going to get a haystack and not sure if there is a needle in there".[379] In addition to this challenge, there is little transparency over the extent of the use of bulk datasets for discovery purposes and few explicit controls in place to ensure adequate protection of individuals' privacy interests.

7.64. The New Zealand situation can be contrasted with that of the United Kingdom and Canada, which have extensive legislative requirements relating to bulk personal datasets. The review is not in a position to reach a view on this issue and, given the work being undertaken by the Inspector-General, would be reluctant to do so in any event. However, it is important that there be enhanced transparency over the extent of the acquisition of bulk datasets for target discovery purposes. Our recommendation is that a ministerial policy statement should set out the Minister's expectations on the acquisition of bulk datasets. We also recommend that the Agencies be required to report in their annual reports on their acquisition of bulk datasets.

---

374 Royal Commission report, part 8, chapter 14 at [60].

375 Royal Commission report, part 7, chapter 2 at [19]. This accords with the approach taken in David Anderson KC *Report of the Bulk Powers Review* (August 2016) at 2-4 (Anderson, 2016).

376 See Anderson, 2016 at 3 footnote 5.

377 New Zealand Security and Intelligence Service *Annual Report 2021* (22 November 2021) at 11.

378 Inspector-General of Intelligence and Security *Annual Report 2022* (November 2022) at 4 and 12.

379 Although we understand that, for discovery purposes, this is often addressed by using publicly available or other minimally intrusive information. As more intrusive activity is generally only appropriate against more specific threats, it would not satisfy necessity and proportionality tests for a 'haystack' dataset for discovery purposes to comprise highly sensitive or other high-risk information.

Necessity and proportionality

The nature of the issue

7.65. When issuing a warrant, the Minister, or the Minister and a Commissioner of Intelligence Warrants as the case may be, must be satisfied that the issue of the warrant will enable the Agencies to carry out an activity that "is necessary to contribute to the protection of national security",[380] or will contribute to international relations and the well-being of New Zealand or its economic well-being.[381] Section 61(a) imposes a requirement that the proposed activity must be necessary to enable the Agencies to perform a function under s 10 or s 11. Section 61 goes on to add two further relevant requirements, namely that:

- the proposed activity is proportionate to the purpose for which it is to be carried out
- the purpose of the warrant cannot be reasonably achieved by a less intrusive means.

7.66. The requirement in s 61(c) that the purpose of the warrant cannot reasonably be achieved by a less intrusive means is one of the components of the proportionality test. Including this component signals that it is important but begs the question why other important components of the proportionality test have been omitted.

7.67. The first issue that arises is that the ISA is not sufficiently explicit as to the approach that ought to be taken to determine whether an activity is 'necessary' and 'proportionate' and therefore justifies the issue of a warrant. The Departmental Report for the Intelligence and Security Bill explained that necessity and proportionality components of what is now s 61 "reflect the key considerations in determining whether a measure constitutes a justified limitation on the rights and freedoms in the New Zealand Bill of Rights Act".[382] There is an argument that it is unnecessary to be more explicit on how an assessment of when an activity is necessary or proportionate is to be made. The contrary view is that, in the absence of more explicit guidance in the ISA, the Minister and Commissioners of Intelligence Warrants have a broad discretion and there is no public reference point to indicate how that discretion might be being exercised.

7.68. The second issue that arises is whether the Agencies should turn their minds throughout an operation to the necessity and proportionality of what they are doing. This would be consistent with the view that an ongoing operation involving the collection of personal information, even if authorised under a warrant, may implicate individual human rights. Therefore, an assessment of necessity and proportionality should expressly apply at appropriate stages during activities authorised under a warrant, not simply at the point at which a warrant is issued.

7.69. To explain our suggestion for more explicit recognition of the necessity and proportionality tests in the ISA, we first describe the legal test from an international human rights perspective, before turning to the New Zealand human rights context. We do so because the international human rights law is more broadly expressed, while New Zealand domestic law is more directly relevant to what the Agencies are obliged to consider.

---

[380] Intelligence and Security Act 2017, s 58(1)(a)(i) and s 60(3)(a)(i).

[381] Section 59(2) and s 60(3)(a)(ii).

[382] Department of Prime Minister and Cabinet, *New Zealand Intelligence and Security Bill: Departmental Report* (8 December 2016) at 28.

The legal test: international human rights

7.70. Under international human rights law, rights such as the right to privacy or freedom of expression, which are the rights most engaged in the context of warrants issued under the ISA, are qualified rights. This means the right is not absolute and may be qualified (or limited) in certain circumstances. The ICCPR, to which New Zealand is a party, sets out the restrictions on those rights that may be permissible. Depending on the right in question, these may include national security or public safety, public order and respect for the rights of others. The Human Rights Committee (established by the ICCPR and charged with monitoring states' implementation of the Covenant) has interpreted whether any restriction is compatible with the Covenant as requiring that the limitation must be provided in law and be necessary for and proportionate to a legitimate aim permitted by the Covenant.[383] We explain this further below.

7.71. Whether an action is necessary has been interpreted as not meaning 'indispensable' but also not 'reasonable' or 'desirable'.[384] This means that there is a high threshold for determining whether an activity is necessary. However, the fact that there are alternatives does not in and of itself mean that an activity cannot meet the 'necessary' threshold.

7.72. Proportionality has been interpreted as requiring that the activity restricting the right be appropriate to achieve their protective functions.[385] The Human Rights Committee has interpreted this as meaning that for an activity to be proportionate, it must be the least intrusive of the measures that might be used and in proportion to the interest to be protected.[386] It must also be justifiable by reference to the precise nature of any threat.[387]

7.73. A further feature of International Human Rights law, which is relevant to both necessity and proportionality, is that any restriction on the rights to privacy and freedom of expression must be in pursuit of 'legitimate aims'.

7.74. Article 19 of the ICCPR (freedom of opinion and expression) refers to the protection of national security, public order or public health or morals as legitimate aims. Article 8 of the European Convention on Human Rights (right to privacy) refers to national security, public safety or the economic well-being of the country (among other things). While Article 17 of the ICCPR (right to privacy) does not stipulate that any restriction on the right to privacy must be necessary for a specified purpose, the view of the United Nations Special Rapporteur on Freedom of Expression is that any restriction should pursue a legitimate aim, which in our view would include the protection of national security.[388]

---

[383] See *General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant)* CCPR/C/21/Rev.1/Add. 13 (26 May 2004) at [6] and *General Comment No. 37 (2020) on the right of peaceful assembly (article 21)* CCPR/C/GC/37 (17 September 2020) at [36].

[384] *Handyside v. the United Kingdom,* No. 5493/72, 7 December 1976 at [48].

[385] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* A/HRS/13/37 (29 December 2009) at [17] (*Special Rapporteur Report*, 2009).

[386] *General comment No. 34: Article 19: Freedoms of opinion and expression* CCPR/C/GC/34 (12 September 2011) at [34]. See also *General Comment No. 27: Freedom of movement (article 12)* CCPR/C/21/Rev.1/Add.9 (1 November 1999(at [14]. And see *Special Rapporteur Report*, 2009 at [17].

[387] *General comment No. 34: Article 19: Freedoms of opinion and expression* CCPR/C/GC/34 (12 September 2011) at [35].

[388] Electronic Frontier Foundation and Article 19 *Necessary & Proportionate: International Principles on the Application of Human rights law to Communications surveillance: Background and Supporting International Legal analysis* (May 2014) at 18. See also *Special Rapporteur Report*, 2009 at [15].

The legal test: New Zealand human rights law

7.75. International human rights provide the broader context for considering how these issues are addressed in New Zealand law. As we noted in chapter 2, the New Zealand Bill of Rights Act 1990 (NZBORA) does not contain an explicit right to privacy.[389] However, the NZBORA's long title states that it is an "Act to affirm New Zealand's commitments to the International Covenant on Civil and Political Rights". Article 17 of the Covenant incorporates the obligation to ensure that no one is subject to "arbitrary or unlawful interference with his privacy, family, home or correspondence" and to ensure that "everyone has the right to the protection of the law against such interference or attacks".[390] There are also other rights in the ICCPR that may be relevant to the implementation of the ISA, particularly Article 19 relating to freedom of expression.

7.76. Privacy underpins s 21 of the NZBORA, which guarantees the right of everyone "to be secure from unreasonable search or seizure, whether of the person, property, or correspondence or otherwise". The Court of Appeal has said that "[t]he main aim of s 21 of the Bill of Rights is to protect privacy interests".[391] It is only where a person's reasonable expectations of privacy have been breached that a personal remedy under the Bill of Rights is available.[392] In this way, the protection of reasonable expectations of privacy is at the core of s 21.[393] In *R v Williams,* the Court of Appeal considered that s 21 should be addressed by first looking at the nature of the privacy interest involved and then undertaking a systematic analysis of the factors that reduce or increase the seriousness of the breach, such as whether it was conducted in an unreasonable manner and whether the response to the particular breach was proportionate.[394]

7.77. Considerations of privacy also arise under s 5 of the NZBORA as a justifiable limitation on rights protected by the Act.[395] Section 5 of the NZBORA allows protected rights to be restricted by such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society. The Supreme Court in *R v Hansen* has indicated that a proportionality inquiry is central to considering whether limitations on rights and freedoms under NZBORA are justified in accordance with s 5.[396] New Zealand courts have stated that an assessment of whether a measure is demonstrably justified involves answering the following questions:[397]

- Does the limiting measure serve a purpose sufficiently important to justify curtailment of the right or freedom?
- Do the means chosen to achieve that objective pass a proportionality test? that is:
  - Is the limiting measure rationally connected with its purpose?
  - Does the limiting measure impair the right or freedom no more than was reasonably necessary for sufficient achievement of this purpose?
  - Is the limit in due proportion to the importance of the objective?

---

389 Submission to the Review, New Zealand Human Rights Commission, April 2022.

390 International Covenant on Civil and Political Rights (ICCPR), Article 17.

391 *R v Williams* [2007] NZCA 52 at [236] per William Young P and Glazebrook J.

392 Above n.

393 *R v Fraser* [1997] 2 NZLR 442 (CA) at 449.

394 *R v Williams* [2007] NZCA 52 at [113-134] per William Young P and Glazebrook J.

395 Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, 2008) at [29].

396 *Hansen v R* {2007] NZSC 7 [2007] at [104] per Tipping J. See also Tipping J at [123] "whether a limit on a right of freedom is justified under s 5 is essentially an inquiry into whether a justified end is achieved by proportionate means."

397 *Four Aviation Security Service Employees v Minister of Covid-19 Response* [2021] NZHC 3012 at [90].

7.78. As we have explained, s 61 of the ISA appears to have sought to codify the necessary and proportionality tests but not in a way that we consider provides the necessary guidance to the issuers or the Agencies.

Other commentary

7.79. Other commentary supports this view. The Law Commission and the Ministry of Justice recommended in their joint report on the Search and Surveillance Act 2012 that a principles section be included in that Act. Issuing officers and enforcement officers would be required to take these principles into account when exercising their powers under the Act. The principles identified by the Law Commission included the principle that state intrusion into an individual's privacy should be proportionate to the public interest in the investigation and prosecution of an offence or the maintenance of the law and that powers under the Act should be exercised in a manner that minimises the level of intrusion on the privacy of any individuals likely to be affected.[398]

7.80. The Human Rights Commission in its submission to the present review referred positively to the joint report on the Search and Surveillance Act. In doing so, it suggested that the review may wish to consider whether the Act should provide for explicit recognition of international human rights obligations[399] and that such explicit recognition might include a set of principles to guide the Agencies in applying necessity and proportionality. Other submitters to the review also supported greater recognition of human rights in the Act.

7.81. The approach by the Law Commission and the Ministry of Justice in the context of the Search and Surveillance Act, and the proposal by the Human Rights Commission in relation to the ISA, are similar to the approach taken by the United Kingdom Investigatory Powers Commissioner's Office (IPCO). The IPCO has issued a notice to guide the Judicial Commissioners in exercising their functions, and this sets out the following questions to guide the proportionality inquiry:[400]

- whether the objective is sufficiently important to justify the limitation of a fundamental right
- whether the measure sought is rationally connected to the objective
- whether a less intrusive measure could have been used
- whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

Our suggested approach

7.82. We do not believe it is necessary to specifically include in the ISA principles against which the necessity and proportionality assessment must be undertaken. We therefore do not recommend that principles be included in the ISA, at least at this time.

---

398 Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC R141, 2017) at [4.44] and [4.57] et seq.

399 Submission to the Review, New Zealand Human Rights Commission, April 2022.

400 Investigatory Powers Commissioner's Office *Approval of Warrants, Authorisations and Notices by Judicial Commissioners* (Advisory Notice 1/2018, 8 March 2018) at [22].

7.83. What we do recommend is that there be some amendment to s 61 to better reflect the approach taken to the application of the necessity and proportionality tests, both within New Zealand and internationally. The specific changes we recommend are as follows:

- The question of necessity should be assessed by reference to the 'legitimate aim', or the s 9 purpose, for which the warrant is being sought, in addition to the functions of the Agencies under sections 10 and 11 of the ISA. This is already the case for warrants that contribute to national security and should be extended to warrants that contribute to international relations and well-being and economic well-being. We consider that although a warranted activity must necessarily relate to the functions of the Agencies, using the functions as a reference point for a necessity assessment is too wide. There will be a more specific reason for seeking a warrant, and it is this purpose not the broader functions of the Agencies that should be the focus of the necessity assessment for all kinds of warrants, not only those for national security purposes.
  - For example, if a warrant is sought for the purposes of contributing to international relations, a justification would need to be provided as to why the warrant is necessary to contribute to international relations, as compared with a justification for why it is necessary to collect and analyse intelligence in accordance with the government's priorities (one of the functions of the Agencies under s 10). This should involve a greater degree of granularity in assessing the purpose of the warrant and whether the warrant is necessary to fulfil that purpose.
- Proportionality should be assessed by reference to the operational objective for which the warrant is being sought. This is the particular objective of the warrant at the operational level. It is not proposed that there be a list of operational objectives from which the most appropriate operational objective is chosen.[401] Rather, the Agencies should identify on a case-by-case basis at the operational level the objective for which the warrant is sought. The reference to an operational objective ensures a degree of specificity in the way proportionality is assessed and can therefore produce more targeted and therefore more appropriate assessments. Of course, depending on the situation, there may be more than one operational objective. For example, intelligence gathering may also involve research and the development of collection techniques. But identifying the operational objective at a greater level of specificity will make it easier to assess whether the use of intrusive powers is reasonable in light of the operational objective.
  - For example, undertaking surveillance activities in respect of an individual who is believed to be acting for a foreign government against New Zealand's essential interests would need to be assessed against the operational objective of ascertaining whether indeed that individual was engaging with that foreign government in that manner.

7.84. We consider that s 61 should be amended to include other relevant components of the proportionality test, including whether the proposed activity is rationally connected to the operational objective of the warrant.

7.85. Although we acknowledge that the Agencies must act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law, we consider the ISA would benefit from a more explicit reference to human rights, and particularly privacy, in section 61. Section 61(d)(ii) currently says that there should be arrangements in place to "minimise the impact of the

[401] As is the situation in the United Kingdom: see Investigatory Powers Act 2016 (UK), s 142(4).

proposed activity on any members of the public". Although this language is broad enough to encompass human rights considerations, it applies only to the impact on any members of the public, not, for example, an individual who may be the target of a warrant. We consider that a specific reference to the privacy considerations arising out of a warrant is appropriate.

7.86. We also believe that the information requirements for a warrant application should support the application of the amended s 61. This means that the Agencies, in addition to the information required to satisfy the issuers that the s 61(d) requirements have been met, should specifically identify the information they consider relevant to the necessity and proportionality assessments and the operational objective of the warrant.

Summary of recommendations – an alternative scheme

7.87. The details of a proposed authorisation framework, which incorporates recommendations made elsewhere in this report, are included in appendix B. In summary, we recommend that the warranting scheme in the ISA be amended as set out below.

RECOMMENDATION: REMOVAL OF TYPE 1 / TYPE 2 WARRANT DISTINCTION 7

Remove the distinction between Type 1 warrants (Intelligence warrant in respect of New Zealanders) and Type 2 warrants (Intelligence warrant in respect of non-New Zealanders) in the Intelligence and Security Act 2017 (ISA).

a. Warrants for the protection of national security in respect of non-New Zealanders should be assessed according to the same criteria that apply to warrants for the protection of national security in respect of New Zealanders.

b. Warrants authorising activities to contribute to New Zealand's international relations and well-being or economic well-being, in respect of New Zealanders, should continue to be assessed against the current criteria in section 59 and the criteria in section 61 of the ISA; warrants authorising activities to contribute to New Zealand's international relations and well-being or economic well-being in respect of non-New Zealanders should continue to be assessed against the criteria in sections 60 and 61 of the ISA.

c. All intelligence warrants should be jointly approved by the authorising Minister and a Commissioner of Intelligence Warrants, who can impose restrictions and conditions on the authorisations.

RECOMMENDATION: APPLICATIONS FOR WARRANTS 8

Update section 55 (Application for issue of intelligence warrant) of the Intelligence and Security Act 2017 (ISA) so that the Government Communications Security Bureau and the New Zealand Security Intelligence Service (the Agencies) are required to provide greater clarity and detail when seeking a warrant and require the following information to be included as part of the warrant application:

a. the purpose of the intelligence warrant applied for

b. the functions to which the warrant relates

c. the operational objective of the warrant and details of the activity proposed to be carried out under the warrant

d. the grounds on which the application is made

e. the arguments for and against the grant of the warrant, including any legal issues that arise in connection with the proposed warrant

f. the information relied on to meet the requirements of section 61 of the ISA (dealing with necessity and proportionality – such as the likelihood of third-party information being collected and the approach that will be taken to data retention, use and disposal)

g. a statement in which the Director-General making the application confirms that all information relevant to the decision whether to issue a warrant that is known to the Agency has been set out in the application and is true and correct

h. if the application is for a renewal or a repeat warrant, the application should specifically address why the authorisation should be continued and the value of the information obtained under the previous warrants.

RECOMMENDATION: DUTY OF CANDOUR 9

Amend section 17 (General duties) of the Intelligence and Security Act 2017 to include an express reference to the duty of candour with which the Government Communications Security Bureau and the New Zealand Security Intelligence Service must act when performing relevant functions.

RECOMMENDATION: WARRANTS TARGETING A CLASS 10

Retain in section 67 (Authorised activities) of the Intelligence and Security Act 2017 (ISA) the ability to obtain an intelligence warrant for a class of persons, subject to:

a. the provision of additional information as part of the warrant application:

   i. A class of persons is defined with as much specificity as possible for the authorisation

   ii. Information is provided on the particular characteristics that the persons in the class share or the common activities in which they are involved

   iii. The process for confirming that an individual falls within the scope of the class is set out in the application, including the criteria to be used and that this is necessary and proportionate

b. further policy work being undertaken with a view to potentially amending the ISA to more clearly identify when it is appropriate to determine that an individual fits within an existing class warrant or where it is appropriate to make a new, specific warrant application in respect of that individual.

RECOMMENDATION: NECESSITY AND PROPORTIONALITY 11

Give greater statutory direction as to how the necessity and proportionality requirements are to be applied:

a. Amend section 61 (Additional criteria for issue of intelligence warrant) of the Intelligence and Security Act 2017 to include that:

   i. the proposed activities authorised under the warrant must be necessary both for the section 9 purpose of the warrant and to fulfil a function of the Government Communications Security Bureau or the New Zealand Security Intelligence Service

   ii. the proposed activity must be proportionate to the operational objective for which it is to be carried out

   iii. the operational objective of the warrant cannot reasonably be achieved by a less intrusive means

   iv. the proposed activity is rationally connected to the operational objective of the warrant

   v. satisfactory arrangements are in place to ensure that individuals' reasonable expectations of privacy in personal information are taken into account.

b. Give statutory recognition to the requirement that an assessment of necessity and proportionality must apply at appropriate stages during the process of undertaking activities authorised under a warrant, not simply at the point at which a warrant is issued.

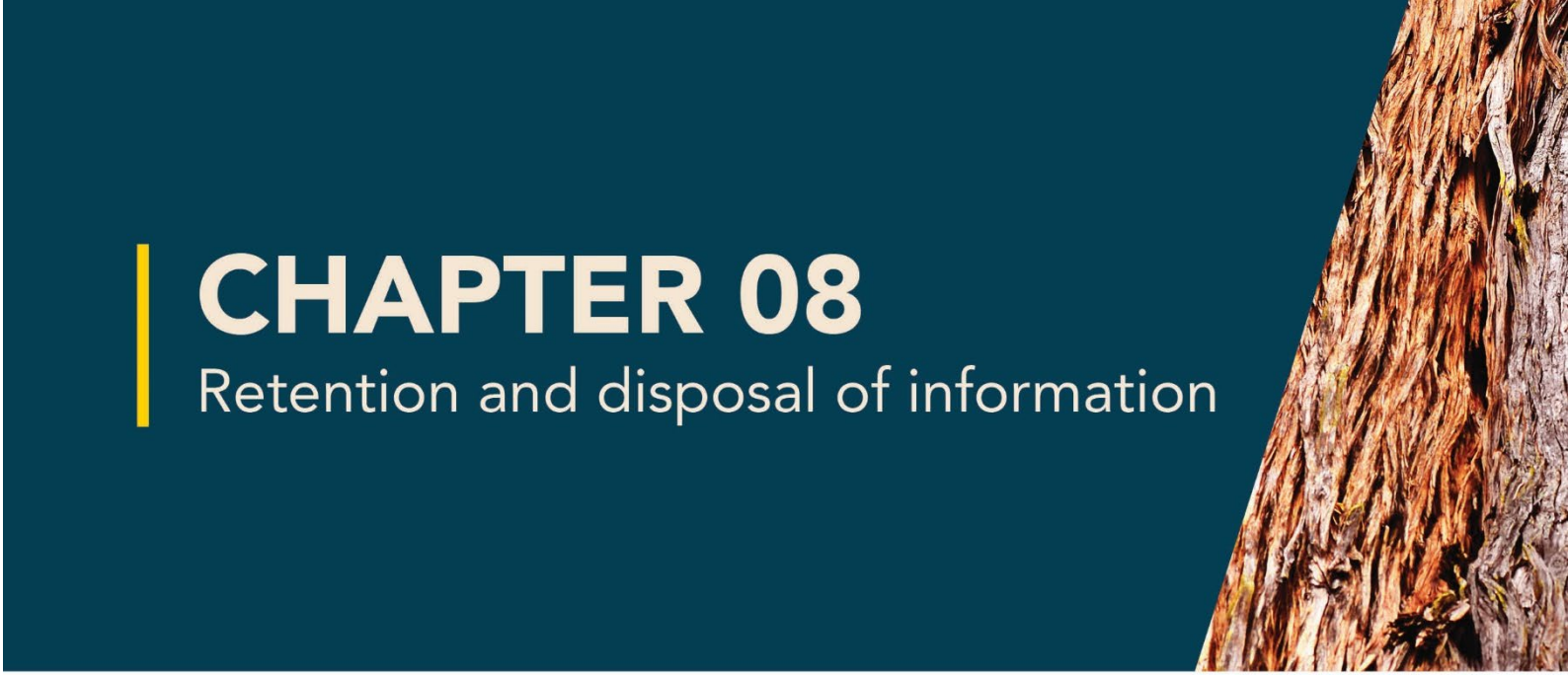
RECOMMENDATION: REPORTING ON THE PURPOSE OF WARRANTS 12

Amend the Intelligence and Security Act 2017 to enhance transparency over the purpose for which warrants are issued and the extent of the acquisition of bulk datasets for target discovery purposes as follows.

a. Amend section 206 (Issue of ministerial policy statements) to include the requirement for a ministerial policy statement on the acquisition of bulk datasets.

b. Amend section 83 (Register of intelligence warrants) to include in the register of intelligence warrants information on the primary purpose under section 9 for which the warrant was issued (eg, national security or international relations and well-being); the function under sections 10, 11 or 12 to which the warrant relates; and where the purpose is the acquisition of bulk datasets.

c. Amend section 221(2)(c) (Annual reports of intelligence and security agencies) to include in the annual report information on the number of applications according to the primary purpose for which a warrant was sought and where bulk datasets are acquired.



CHAPTER 08
Retention and disposal of information

Introduction

8.1. Intelligence and security agencies are in the business of information: the collection of information; the examination, analysis and use of information; and the retention and disposal of information.[402] Provisions on the retention and disposal of information collected by intelligence and security agencies are among the safeguards that can be applied to balance individual rights with the needs of either national security or the other purposes provided for in the Intelligence and Security Act 2017 (ISA). The terms of reference for this review state that it should have particular regard to:

> whether the ISA adequately provides, and has appropriate protections and oversight in place, for .... The processing, analysis, retention and destruction of collected information/data.

8.2. Taking this into account, this chapter commences by looking at the context for the retention and disposal of information in light of the information explosion in the internet age.

8.3. It goes on to consider the existing legal framework for retention and disposal of information set out in the ISA and how those requirements have been implemented by the intelligence and security agencies (the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) and referred to in this report as 'the Agencies').

8.4. The issues with the provisions of the ISA are then identified. These centre on the requirements to destroy irrelevant information and the challenges that can arise in making that assessment, especially in a discovery context. Factors considered are information that is collected for one purpose but may have a use for another purpose, the privacy interests in the protection of personal information, privileged information, retention of information for oversight purposes, retention for archiving purposes and the declassification of information.

8.5. To be effective, the framework for the retention and disposal of information must be workable and there must be transparency in how the Agencies manage the information they acquire. There is also a requirement to hold information in a manner that enables effective oversight as well as for other statutory purposes. This chapter looks at these issues as well as the balance between the need to retain information for national security and other ISA purposes and the need to dispose of information, particularly personal information, that is not related to those

[402] We note that in this chapter we refer to the retention and 'disposal' of information. This is broader than the destruction of information, which is referred to in paragraph 2.4 of the terms of reference. It includes, for example, the transfer of information for archiving purposes.

purposes. In doing so, it also responds to another of our terms of reference: "whether the Act appropriately balances national, community and individual security with individual privacy and other rights".

Retention and disposal of information in the internet age

8.6. We live in an era of constant and rapid technological change. As we outlined in chapter 2, people's daily activities are increasingly being conducted through online information infrastructure, including mobile phones and other internet connected devices. It is estimated that by 2025, 463 exabytes (463 billion gigabytes) of information will be generated each day globally on the internet.[403] This poses both challenges and opportunities. Criminals and malicious actors who would do harm to Aotearoa New Zealand's national security may use the internet for criminal and subversive activities, while hiding their identities and actions. Law enforcement and intelligence agencies seek to use information from the internet to assist in the investigation of criminal activity as well as to identify threats from terrorism and violent extremism, foreign interference and cyber-attacks on critical infrastructure. Digital information helps to identify these threats, to ascertain their source and to mitigate them.

8.7. In this environment, electronic data is vitally important. The online environment has changed the way information is managed, stored, retained and destroyed. The mass of information available on the internet is so great that it is beyond the capacity of individuals to process every digital record and decide what to keep and what to destroy. Automated rules and algorithms for these purposes are increasingly important.

8.8. The ISA must be capable of keeping up with this rapid technological change. In this environment, it is no longer viable to consider information as discrete pieces of information, much like pieces of paper. While information may take this form, it frequently takes the form of metadata. For example, electronic call associated data includes the sender or recipient of a communication, the time and duration of the communication, the communications system and its location. Internet connection records include source IP address, destination IP address, time and date, volume of data transferred and the name of the internet service or server that has been connected to. Metadata may be as valuable for intelligence purposes as content data. An individual piece of information may be irrelevant on its own, but it may gain in significance in light of its wider context. For example, the purchase of a gun may not be particularly enlightening on its own, but combined with other pieces of information, such as espousing violent extremist views, it may take on a different complexion. Furthermore, communications information is transient and can be lost as quickly as it appears.

8.9. An information retention framework is a tool to enable intelligence and security agencies to achieve their objectives. It is an integral part of the end-to-end process of the intelligence cycle, as described in Diagram 1 of chapter 6. In chapter 7, we discussed human rights considerations with respect to the collection of intelligence through warranting processes. Safeguards, such as the application of the necessity and proportionality tests, do not apply just to the warranting process. They apply throughout the intelligence cycle, including the retention and disposal of data.

8.10. A retention and disposal framework must therefore allow an intelligence and security agency the ability to retain the information it requires to meet operational objectives, while also protecting the interests of those who are not of intelligence and security interest by requiring the prompt

[403] S Barrett "How Much Data Is Produced Every Day in 2022" (30 May 2021) The Tech Trend <https://the-tech-trend.com>.

disposal of their information. There is, of course, a balance to be struck between data retention requirements that are too constraining and affect the extent to which the Agencies can pursue their legitimate security intelligence functions and ones that are too liberal and potentially threaten the legitimate privacy interests of individuals who pose no threat to national security.

Privacy interests in personal information

8.11. There is a legitimate interest in ensuring that the Agencies do not retain and use personal information in a manner that unduly infringes privacy interests. These interests extend beyond the collection of information to its retention, examination, use and disclosure.

8.12. Section 22 of the Privacy Act 2020 sets out the privacy principles that are applicable to the Agencies. Because of the covert nature of the Agencies' activities, some of the privacy principles are not applicable.[404] However, the following information privacy principles are relevant to the Agencies:

- Information privacy principle 1 clarifies that personal information must not be collected by an agency unless the information is collected for a lawful purpose connected with a function or an activity of the agency; and the collection of the information is necessary for that purpose.
- Information privacy principle 9 provides that an agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.
- Principle 10(2) provides that an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a secondary purpose) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.
- Information privacy principle 11(1)(g) provides that an agency that holds personal information must not disclose the information to any other agency or to any person unless the agency believes on reasonable grounds that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions.

8.13. We set out these information privacy principles here as part of the framework for considering the ISA's approach to retention and disposal of information and will return to them later in this chapter.

Legal framework for retention and disposal of information

8.14. The ISA provides some of the framework for the retention and destruction of information. This is supplemented by a ministerial policy statement (MPS) and other legislation: the Privacy Act 2020, the Official Information Act 1982 and the Public Records Act 2005. The following is a summary of the requirements:

- Information unintentionally obtained outside the scope of a warrant or authorised activity must be destroyed immediately unless an intelligence warrant is issued that authorises its

[404] According to s 28 of the Privacy Act 2020, information privacy principles 2, 3 and 4(b) do not apply to an intelligence and security agency.

collection or it is disclosed for certain purposes.[405] Any such warrant must be obtained as soon as practicable.

- There is an obligation to destroy all other lawfully collected but irrelevant information as soon as practicable. Irrelevant information is information that is not required (or no longer required) by an Agency for the performance of its functions.[406]
- Information that is incidentally obtained (ie, obtained during the exercise of functions but not relevant to those functions)[407] may only be retained for the purpose of disclosing it to another agency (eg, Police) in limited circumstances, such as preventing or detecting serious crime or preventing threats to life or to the security and defence of New Zealand.[408]
- Information obtained under an urgent or very urgent authorisation must be destroyed as soon as practicable if that authorisation is subsequently revoked unless it is retained for the purpose of disclosing it to another agency in limited circumstances.[409]
- All business records information obtained under a business records direction must be destroyed as soon as practicable if the records are irrelevant to the performance of an Agency's functions unless retention is required by any other laws or court orders.[410]

8.15. The MPS on information management is dated 1 March 2022 and provides further guidance on the management of information, including its retention and disposal. The MPS applies to all information obtained, collected, created and/or managed by the GCSB and the NZSIS in the course of exercising their statutory functions. It includes information intercepted, seized, copied or otherwise obtained under a warrant or authorisation or other lawful means that do not require a warrant. In dealing with this information, it requires employees of the agencies to have regard to:

- necessity and proportionality
- security of information
- privacy protection
- shared responsibility
- oversight.

8.16. The MPS also notes that all government agencies are subject to legislative requirements under the Public Records Act 2005, the Privacy Act 2020 and the Official Information Act 1982 to retain, protect and, where appropriate, provide access to information.

8.17. The MPS requires that the general principles it sets out are to be supplemented by guidelines to assist the Agencies' employees to determine whether information is required for the performance of statutory functions – either immediately or in the longer term.[411] The policies and processes on the retention and destruction of information are aimed at helping the Agencies to make the judgement necessary to identify and destroy unauthorised and/or

---

[405] Intelligence and Security Act 2017, s 102.

[406] Section 103.

[407] "Incidentally obtained information" is defined in s 47 of the ISA as information that a) is obtained in the course of performing a function under section 10 or 11; but b) is not relevant to either of those functions.

[408] Intelligence and Security Act 2017, s 104.

[409] Sections 76 and 81.

[410] Section 152.

[411] Minister Responsible for the GCSB and NZSIS *Ministerial Policy Statement on Information Management (MPS on Information Management)* (online, 1 March 2022) at [19].

irrelevant information and to retain other information. This is information that has been determined as required for as long as it remains required for a business purpose related to a statutory function, or is required to be retained as a public archive. The guidelines also provide indicative timeframes in which the above determinations must be completed. The MPS provides for the specification of retention periods and, where information has reached the end of any retention timeframe, for its destruction or continued retention if that is justified on grounds of necessity and proportionality.[412]

8.18. The Agencies both have policies for addressing data access, management, retention and destruction. These are classified and therefore not available for public scrutiny (although they are subject to the Inspector-General of Intelligence and Security's (Inspector-General) scrutiny). These policies follow the requirements of the MPS and set out the processes for the retention of data that are consistent with the ISA and include the timeframes for data retention and destruction.[413]

8.19. There has been a mixed assessment of the efficacy of the requirements for the retention and disposal of intelligence. In the 2020 annual report, the Inspector-General indicated that "assurance that the agencies retain only what is necessary for them to perform their functions, and dispose of what is not, depends on a combination of policies, procedures and technology".[414] A year later in the 2021 annual report, he referred to ongoing issues with the Agencies' data retention and destruction policies and commented that the Agencies' approach to data destruction and retention was "slow to develop".[415] However, in December 2021, the GCSB adopted a new data retention and destruction policy. The new policy better reflects the way the GCSB and its systems and processes function and applies default retention time limits. In the 2022 annual report, the Inspector-General advised that this "new policy appears to be an improvement on the old".[416] In the same report, the Inspector-General also recognised that the NZSIS was developing its systems and processes.

Information collected outside of the scope of a warrant (section 102)

8.20. Warrants authorise the collection of specified information, such as intercepted communications of a particular individual. However, on occasion, the Agencies may unintentionally collect information that does not fall within the scope of the authorisation or authorised activity but the information is still relevant to the Agencies' functions. For example, the Agencies may be authorised to intercept the communications of person A. If person A communicates with, or about, person B, then that information is authorised and may be collected within the scope of the warrant. However, if the Agencies unintentionally overhear person B's communications to someone other than person A, then that is unauthorised.

---

412 Above n, at [30]–[31].

413 Other legislative requirements are also relevant to information collected by the agencies. Key among these are the Official Information Act 1982, the Privacy Act 2020 and the Public Records Act 2005.

414 Inspector-General of Intelligence and Security *Annual Report for the year 1 July 2019 to 30 June 2020* (26 January 2021) at 6.

415 Above n, at 7.

416 Above n.

8.21. In these circumstances, s 102 applies. Section 102 provides as follows:

> **Destruction of unauthorised information**
>
> (1) In this section, unauthorised information means—
>
> (a) information unintentionally obtained that is outside the scope of—
>
> (i) an authorisation; or
>
> (ii) an authorised activity; or
>
> (b) information obtained during the provision of co-operation, advice, and assistance under section 14 that could otherwise only be obtained during the carrying out of an authorised activity.
>
> (2) Unauthorised information must be destroyed immediately after it is obtained unless,—
>
> (a) on an application that is made as soon as practicable, an intelligence warrant is issued authorising collection of the information; or
>
> (b) section 104 applies.

8.22. Concerns have been raised in this review by the Agencies over the workability of s 102 of the ISA. Some specific drafting issues have been raised.

- First, the 'immediacy' of the destruction requirement is not practical. It does not allow sufficient time for the Agencies to determine whether the information has sufficient intelligence value to justify applying for another warrant or to decide whether s 104 (relating to disclosures of incidentally obtained information) may apply. A timeframe such as 'as soon as practicable' would be more workable.
- Second, some technical drafting issues were raised with us. Section 102(1)(a) provides that information "**unintentionally** obtained that is outside the scope" of an authorisation must be destroyed. The use of 'unintentionally' might perhaps imply that information that is **intentionally** obtained that is outside the scope of an authorisation does not need to be destroyed.
- Third, unauthorised information must be destroyed unless an 'intelligence warrant' is issued authorising the collection. This does not specifically enable urgent or very urgent authorisations to be issued authorising the collection.

8.23. We agree that making the first and third of these changes is appropriate and that s 102 should be amended to provide that unauthorised information should be destroyed 'as soon as practicable' rather than 'immediately', and s 102(2)(a) should be expanded to cover urgent and very urgent authorisations.

8.24. We do not agree that any issue arises through the inclusion of 'unintentionally' in s 102(1)(a). We see no reason for removing the word 'unintentionally', and, indeed, see potential risks in doing so.

8.25. A further issue that has arisen is that s 102 turns on an assessment as to what is inside or outside the 'scope' of an authorisation or authorised activity. However, there is a lack of clarity provided by the ISA, and different interpretations, as to what may be within or outside the scope of an authorisation.

8.26. The reference to the "scope of an authorisation" in what is now s 102 was added at the select committee stage of the New Zealand Intelligence and Security Bill. The clause had up until then referred only to unauthorised information as information "outside the scope of an authorised activity". The departmental report expressed concern that this might mean that intelligence unintentionally collected about a New Zealander under a Type 2 warrant would be within the scope of an authorised activity and be able to be retained, which was not the intention. The departmental report recommended that the clause refer to the 'scope of an authorisation'.[417] As a result, this was added to the clause alongside "scope of an authorised activity". The effect of this change (and, indeed, its intention) was to narrow the circumstances in which unintentionally obtained information may be retained without a further authorisation.

8.27. As noted, there are differing interpretations of what would be included within the 'scope' of an authorisation.

- There is an argument that the scope of an authorisation covers all the matters required to be stated in an intelligence warrant under s 66. This includes the purpose for which the warrant is obtained. The consequence of this interpretation is that information obtained under an authorisation for one purpose, but which relates to another purpose, would have to be destroyed under s 102, or another authorisation would need to be sought, even if information obtained was necessary for that other purpose.
- An alternative view is that the scope of an authorisation should be determined by reference to the person or class of persons in respect of which the warranted activity is being carried out. This means that, as long as the information relates to the person that is the subject of the warrant, it will be within scope and s 102 would not apply. Such an approach would be consistent with information privacy principle 10(2) that personal information obtained by an Agency in connection with one purpose may be used for a secondary purpose if the use of the information for that purpose is necessary to enable the Agency to perform any of its functions.

8.28. What is and what is not outside the scope of an authorisation is crucial to determining which information must be destroyed, except if another warrant is sought or s 104 applies. Our view is that the legislators intended there to be a difference between the scope of an authorisation and the scope of authorised activities. We do not consider that any differences in interpretation can remain unresolved. Clarification of the meaning of 'scope of authorisation' is required.

The relevance and irrelevance of information (s 103)

8.29. Section 103 of the ISA outlines what the Agencies must do if they collect 'irrelevant' information under a warrant.

> **Destruction of irrelevant information**
>
> (1) In this section, irrelevant information means information that—
>
> (a) is obtained by an intelligence and security agency within the scope of an authorised activity; but
>
> (b) is not required, or is no longer required, by the agency for the performance of its functions.

[417] Department of Prime Minister and Cabinet, *New Zealand Departmental Report to the Foreign Affairs and Trade Committee*, December 2016 at [646].

> (2) Irrelevant information must be destroyed as soon as practicable.
>
> (3) Subsection (2) is subject to—
>
> (a) any enactment requiring the retention of the information; or
>
> (b) any order of a court that imposes a prohibition on the destruction of the information.

8.30. In other words, s 103 requires the Agencies to assess the relevance of information, and when something is found to be irrelevant (ie, not required or no longer required for the performance of an Agency's functions), it must be destroyed as soon as practicable.

8.31. The Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 Mach 2019 considered that there were potential issues with this provision of the ISA and suggested that it be reviewed.[418] It pointed out that the section assumes that relevance and irrelevance are binary concepts and that the Agencies are able to continuously monitor the relevance of information. It considered that neither assumption is correct and furthermore the resources required for ongoing monitoring of relevance would impact on the Agencies' abilities to carry out other important functions.[419] The Inspector-General has also suggested that the ISA requirement to destroy irrelevant information as soon as practicable is problematic for an intelligence agency, as data can be valued for its possible relevance in the future.[420]

8.32. We agree that the use of 'relevance' to define whether information collected under warrant should be retained or destroyed is problematic. According to s 103, deciding whether information is relevant or irrelevant means determining that the information is not required or no longer required for the performance of the Agencies' statutory functions. This is difficult to determine, not only at any one point in time, but also over time. Information may be of future value, but it may be impossible to determine in advance whether it **will** be of future value. Thus, the basic premise of s 103 – that it is possible to determine at the time a decision is taken whether information may be required in future – does not hold. As pointed out by the Royal Commission, it implies an ongoing determination of whether the information continues to be required for the performance of the Agencies' functions.

8.33. This suggests that a different approach is needed. The United Kingdom looks at the same issue of whether to retain or destroy information collected under certain types of warrants by examining the purposes for which the warrant may be granted in the first place. Thus, retention must be necessary for any of the purposes for which a warrant may be granted or for the exercise of oversight functions and public records archiving.[421]

8.34. Requiring that information obtained under a warrant is destroyed unless its retention is necessary to fulfil a purpose for which a warrant may be authorised, as well as to fulfil the functions of the Agencies, ensures that both an authorisation for the collection of intelligence and the retention of the information that is collected meet the same necessity requirements. Thus, if a warrant may be issued for one of the purposes set out in s 9 of the ISA, such as for the protection of national security, and if the retention of information obtained within the scope of

---

[418] *Royal Commission of Inquiry Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) at part 8, chapter 14, [116]–[118] (Royal Commission report).

[419] Royal Commission report, above n at [117].

[420] Inspector General of Intelligence and Security *Annual Report for the year 1 July 2020 to 30 June 2021* (11 November 2021) at 8.

[421] Investigatory Powers Act 2016 (UK), s 53, s 129, s 152.

an authorised activity is necessary to meet one of those purposes and to fulfil the functions of the Agencies, the information may be retained. If not, the information must be destroyed.

8.35. The use of the comparable necessity test as in the application for the warrant should facilitate the practical application of decisions to retain information without requiring re-assessment on an ongoing basis of whether retention may still be required to fulfil a function of the Agencies.

8.36. In addition to maintaining the reference in the Agencies' policies to specific retention periods for various classes of information, we consider that information obtained under a warrant should be reviewed at specified intervals to confirm that the justification for its retention is still valid.[422] If information is no longer necessary for a purpose for which a warrant may be issued or to fulfil the functions of the Agencies, it must be destroyed. This means, for example, that if information is collected under warrant on an individual who was assessed to be of national security concern, but who turns out **not** be of national security interest after all, then unless otherwise required for a statutory purpose, that information must be destroyed as soon as practicable after the assessment is made.

8.37. The aim of this approach is to enhance the guidance given to the Agencies on how to make assessments of the future value of information. The intervals for assessment of information to determine whether its retention remains necessary should be set out in policy documents. Furthermore, the assessment requirement should be robustly implemented to avoid the retention of information 'just in case' it might be useful in future.

Time period for retention of information

8.38. We consider that for transparency purposes, there should be clear rules around retention periods for various classes of information.

8.39. As part of our engagement process, we asked members of the public how long Agencies should be able to keep information collected under a warrant if it is irrelevant to its work now, but could possibly be important in the future. A majority of respondents indicated that it was acceptable for the Agencies to keep information for some length of time, but the time period was unclear (respondents selected either one year or ten years). Also, approximately one-third of participants thought this information should not be kept at all. It is therefore difficult to draw conclusions from the public engagement process on the length of time the public considers information should be retained.

8.40. The retention periods for various classes of information are currently set out in policy documents, as required by an MPS. We consider that dealing with time periods for the retention of information in the relevant MPS remains the best approach. The MPS should therefore continue to require the Agencies to specify retention periods for various classes of information, and this should include information obtained under warrant, information obtained from partners and unsolicited information.

Retention of information for oversight and maintenance of public records

8.41. The requirement in s 103 to destroy irrelevant information is subject to any enactment that requires the retention of information. This is a reference to the Public Records Act 2005. Disposal Authority 692 issued by the Chief Archivist applies to GCSB, NZSIS and the National Security Group of DPMC. It sets out minimum retention periods and disposal actions, sometimes by

[422] This is the approach adopted by the United Kingdom in the *Interception of Communications: Draft Revised Code of Practice* (October 2022) at [9.23] and [9.24].

reference to internal GCSB and NZSIS policies, for various classes and sub-classes of information, including information and records created and received as part of the gathering, analysis and assessment of intelligence.

8.42. One of the purposes of the Public Records Act is to enable the government to be held accountable by providing for the preservation of, and public access to, records of long-term value. An issue was raised with us by the Ombudsman over the Agencies' approach to declassification and public release of their records. It was suggested that the review might consider whether the ISA should reflect the need for the public sector to have the infrastructure necessary to support systematised and ongoing declassification.

8.43. The NZSIS is working on an archives release programme to progressively transfer files to Archives New Zealand. Some transfers have taken place, including files relating to the 1951 Waterfront Dispute and the 1970s' William Sutch papers. It appears from the NZSIS website that no files have been declassified and transferred since 2010.[423] In part, this may be because resources available for declassification are limited. We have been advised that the NZSIS is currently undertaking a declassification 'proof of concept' project to determine necessary resources, requirements and priorities, with the objective of making as many as possible of the NZSIS's historical records publicly available. Declassification and making information available to the public is important for government accountability. Adequate resources should be dedicated to this task, especially in light of the otherwise secret nature of the intelligence and security activities.

8.44. Finally, there is a legislative gap in that the destruction obligation in s 103 is not subject to any requirement to retain information in order to facilitate review by the Minister responsible, the Commissioners of Intelligence Warrants, the Inspector-General and the Intelligence and Security Committee for the purposes of oversight. This is a gap that should be rectified so that information required for the purposes of a review as part of the exercise of oversight functions can be retained, and in the circumstances where information has been destroyed, a record of this should be kept.

Incidentally obtained information (s 104)

8.45. Section 104 deals with information that is incidentally obtained: That is information collected by the Agencies when they are performing their intelligence collection and analysis or protective security services, or advice and assistance functions, but which is not relevant to those functions. For example, the Agencies may obtain information indicating that an armed robbery is being planned. Such information may only be disclosed in one of the limited circumstances set out in s 104(3).

8.46. Under s104(3), disclosure may be made to the Police, the New Zealand Defence Force (NZDF) and "any public authority (whether in New Zealand or overseas) that the Director-General considers should receive the information" where the Director-General has reasonable grounds to believe the disclosure of information may assist in:

- preventing or detecting serious crime[424]
- preventing or responding to threats to the life of any person

[423] NZSIS "Records and Archives" Te Pā Whakamarumaru New Zealand Security Intelligence Service <nzsis.govt.nz>.

[424] Serious crime is defined as any offence punishable by two or more years of imprisonment.

- identifying, preventing or responding to threats or potential threats to security or defence
- preventing the death of any person who is outside the territorial jurisdiction of any country.[425]

8.47. The Inspector-General considered the implementation of s 104 in his report on a review of the NZSIS framework for disclosing incidentally obtained information on crime to the Police.[426] He gave general support to the discretion, which may be exercised by the Director-General of the NZSIS in deciding whether to disclose to Police information on serious crime that is incidentally obtained through intelligence operations.[427] The Inspector-General suggested a number of factors that the Director-General may take into account in decision-making,[428] as well as a number of other recommendations.[429] These suggest that the threshold for disclosure is high. They could be considered by the Agencies as appropriate guidance or operational policy on the implementation of s 104.

8.48. Domestic agencies in the wider intelligence community have asked us whether the closed list of circumstances identified in s 104(3) should be expanded to account for a broader range of threats and behaviours that could result in significant risk to broader national security interests. This could include, for example, circumstances where disclosure would assist to protect the 'safety' of New Zealanders beyond preventing or responding to threats to life or to protect against threats to New Zealand's infrastructure or biosecurity.

8.49. The disclosure of information under s 104 concerns information that has been incidentally obtained, and therefore, there should be controls over its disclosure. We consider that the reference to 'threats or potential threats to the security or defence of New Zealand' should be sufficient to cover most of the other situations where disclosure would be warranted. We are therefore not convinced that the circumstances warranting disclosure should be broadened.

8.50. In any case, s 104 permits the disclosure of incidentally obtained information to the Police, NZDF and "any public authority (whether in New Zealand or overseas) that the Director-General considers should receive the information". The scope of s 104 would therefore cover other New Zealand agencies with a law enforcement role, such as New Zealand Customs and the Ministry of Primary Industries. However, for transparency purposes, the ISA could include a specific reference to those other enforcement agencies for which information, for example, on transnational organised crime, would be valuable for the exercise of their enforcement functions.[430]

---

[425] Intelligence and Security Act 2017, s 104(3)(a-d).

[426] Inspector General of Intelligence and Security *Review of NZSIS framework for disclosing incidentally obtained information on crime to the Police* (20 December 2021).

[427] Above n, at [40].

[428] Above n, at [41].

[429] Above n, at [45]–[52].

[430] We recognise that s 13 of the ISA provides for the Agencies to cooperate with the Police and Defence Force in the exercise of those agencies' functions and not other domestic agencies with a law enforcement function. However, s 104 already provides for the possibility of disclosure to other public authorities.

RECOMMENDATION 13

Amend sections 102 to 104 (Destruction and retention of information) of the Intelligence and Security Act 2017 (ISA) to make them fit for purpose.

a. Amend section 102(2) (Destruction of unauthorised information) to replace the reference to "unauthorised information must be destroyed immediately" with "unauthorised information must be destroyed as soon as practicable".

b. Amend section 102(2)(a) to include the issuance of urgent intelligence warrants and very urgent authorisations, in addition to "intelligence warrants", as exceptions to the requirement to destroy unauthorised information.

c. Clarify the interpretation of what is and what is not "outside the scope of an authorisation" in section 102 of the ISA.

d. Amend section 103 (Destruction of irrelevant information) to remove the reference to "irrelevant information" and replace with a requirement to destroy information collected within the scope of an authorised activity unless its retention is necessary for a purpose for which a warrant may be granted and to fulfil the functions of the Government Communications Security Bureau and the New Zealand Security Intelligence Service.

e. Amend section 103(3) to add a proviso that the destruction of information is subject to retention where it is required to enable the exercise of the functions of an oversight body, or if it has been destroyed, then a record of this is kept.

f. Amend section 104(2) (Retention of incidentally obtained information) to explicitly name the agencies in New Zealand, in addition to the New Zealand Police and New Zealand Defence Force, with enforcement powers, including the New Zealand Customs Service and Ministry for Primary Industries, with which the Agencies may share incidentally obtained information, while still retaining the ability for the Director-General to determine whether any other public authority should receive the information.

RECOMMENDATION 14

Provide additional resources to the Government Communications Security Bureau and the New Zealand Security Intelligence Service to enable them to declassify information for preservation with Archives NZ, given the importance of public records for Government accountability.

Privileged information

8.51. Existing controls under the ISA address the collection of privileged information. Under s 70, an intelligence warrant may not be sought for the purpose of obtaining "privileged communications or privileged information" of a New Zealand citizen or permanent resident. "Privileged communications or privileged information" is defined in terms of legal professional privilege, privilege attaching to ministers of religion and medical privilege in the context of criminal

proceedings. It does not cover journalists, their confidential sources and the communications of Members of Parliament. The departmental report on the New Zealand Intelligence and Security Bill 2016 noted:[431]

> In terms of protection for communications with Members of Parliament and journalists and their sources, the Bill does not confer a clear prohibition in relation to such communications. However, clause 3 [now ISA, s 3] makes clear that the primary purpose of the Bill is the protection of New Zealand as a free and democratic society. All of the provisions of the Bill will need to be given effect in light of this … It would be an exceptionally high bar to target a Member of Parliament or a journalist.

8.52. The operation of s 102 means that any privileged communications or privileged information must be destroyed and not retained, used or disclosed, unless the tests for disclosure under s 104 apply. The MPS on the management of information requires the Agencies to have policies in place to address the need to protect privileged information and to apply protections, including the obligation to destroy (without reporting) any privileged material relating to New Zealanders that is unintentionally obtained or collected.[432] The MPS also requires that the Agencies give additional protection to information that relates to 'sensitive category individuals', including Members of Parliament, members of the New Zealand judiciary and journalists.[433] A joint policy statement of July 2021, a summary of which has been released under the Official Information Act, requires that any activity involving a sensitive category individual or their information is lawful, necessary and proportionate.[434]

8.53. Three issues have arisen with respect to privilege:

- whether the retention of incidentally obtained information applies notwithstanding the privilege protections in s 70 of the ISA
- whether the disclosure of privileged information under s 104 should be significantly restricted in line with the nature of privileged communications
- whether s 70 of the ISA should be broadened to include privileged material obtained or received other than under warrants.

8.54. First, there is an issue over whether s 104, relating to the retention of incidentally obtained information, applies notwithstanding the privilege protections in s 70 of the ISA. This was one of the issues raised in a 2018 Inspector-General review of New Zealander's privileged communications and privileged information.[435] The Inspector-General considered that where the limited exception in s 104 applies, the material should be destroyed after disclosure, and clear record-keeping requirements should be established, but without identifying the privileged material at issue.[436] We agree that in order to enhance oversight over the application of s 104, a register of disclosures under s 104 should be kept. The retention and destruction of information under s 104

---

[431] Department of the Prime Minister and Cabinet *Departmental Report New Zealand Intelligence and Security Bill* (online, December 2016) at [593].

[432] Minister Responsible for the GCSB and NZSIS *Ministerial Policy Statement – The management of information by GCSB and NZSIS, including retention and disposal of that information* (1 March 2022) at [32].

[433] Above n, at [37].

[434] GCSB and NZSIS *Joint Policy Statement: JPS – 013 Making a Protected Disclosure* (Release under Official Information Act request).

[435] Inspector-General of Intelligence and Security *A review of the New Zealand Security and Intelligence Service's handling of New Zealanders' privileged communications and privileged information* (online, December 2018).

[436] Above n, at [29].

should form part of the Agencies' regular audit programmes and could also be subject to periodic auditing by the Inspector-General.

8.55. The second issue we have considered is whether disclosure of unintentionally acquired privileged information that falls within s 70 of the ISA should be subject to a higher disclosure threshold than is set out in s 104. We note that cl 8.2 of the rules for conduct and client care of lawyers sets out the circumstances in which lawyers are required to disclose confidential client information.[437] Those circumstances are similar to the circumstances set out in s 104(3). Accordingly, we do not consider that a higher threshold is required. If disclosed under s 104, the privileged information should be destroyed after disclosure and a record of this kept for oversight purposes.

8.56. A third issue was raised by the Inspector-General, namely that s 70 prohibits an intelligence warrant from authorising the exercise of any power for the purpose of obtaining privileged communications or privileged information of a New Zealand citizen or permanent resident but does not address privilege in unsolicited information.

8.57. Privilege protects the confidentiality of the communications made in an atmosphere of trust between the parties. The protection of legal professional privilege falls under Article 14 of the International Covenant on Civil and Political Rights (ICCPR) on the right to a fair trial. Other privilege is protected by Article 19 of the ICCPR on freedom of expression. The protection of journalists' sources is related to the right to freedom of expression.[438] There is a significant public interest in the dissemination of information by journalists "and hence in the need to protect the confidentiality of the sources from which journalists obtain information".[439] As we have already explained, the ISA requires the Agencies to act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law. In addition, the ISA sits together with the common law on privilege, including legal professional privilege.

8.58. We are not convinced of the need to amend s 70 when it is read in conjunction with the other requirements of the ISA and with the common law, and noting the Agencies internal policies providing guidance on these issues. To the extent that there are any remaining issues, including with respect to privilege in unsolicited information and the protection of journalists' sources, we suggest that these be addressed in a revision to the relevant joint policy statement and that this revision be expedited.

A framework for the retention and destruction of all lawfully collected information

8.59. In this chapter, we have discussed some of the specific issues that have arisen in relation to the ISA and retention and destruction of information. The ISA has provisions at s 102 to s 104 for information collected under a warrant that is unintentionally obtained outside the scope of a warrant, is irrelevant information or is incidentally obtained information. The ISA also requires the Agencies to ensure information obtained in reliance on an intelligence warrant will be retained, used and disclosed only in accordance with the ISA or other enactment[440] and mandates the issue of a MPS on the management of information obtained by an Agency,

---

437 See the schedule to the Lawyers and Conveyancers Act (Client Care Rules) 2008.

438 *General Comment No. 34 on Article 19: Freedoms of opinion and expression* CCPR/C/GC/34 (12 September 2011) at [45].

439 *Hager v Attorney-General* [2016] 2 NZLR 523 at [88].

440 Intelligence and Security Act, s 61(d)(iii).

including the retention and destruction of that information.[441] The ISA does not otherwise provide for information that is lawfully obtained by the Agencies (under a warrant or authorisation and other lawful means), and that is necessary for the purposes of national security, international relations and well-being, economic well-being or to fulfil the functions of the Agencies.

8.60. Without providing a framework for the retention and destruction of all lawfully obtained and necessary information, the ISA does not provide the desired transparency regarding the controls that are in place on the management of information, and its retention and disposal. Neither does it ensure that the retention, use and disclosure of personal information is subject to safeguards consistent with the information privacy principles of the Privacy Act 2020.

8.61. We believe there should be a framework in the ISA for the retention and disposal of all information obtained, collected, created and/or managed by the Agencies in the course of exercising their statutory functions. This includes information that is obtained under a warrant or authorisation, as well as other lawful means. It would build on the provisions at s 102 and s 104, while fundamentally replacing the provisions at s 103.

8.62. We have already set out our specific recommendations regarding the retention and disposal of information obtained under warrant. More generally, we agree with the MPS that information management policies should apply throughout the intelligence cycle. In managing information, Agency employees are required to have regard to necessity and proportionality, as well as other factors such as privacy protection and oversight.

- We consider that the application of the necessity and proportionality tests, including where they relate to the retention and disposal of information, should be rigorous and specific. Necessity and proportionality tests should be applied throughout the process of examination, use, retention and disposal of information.
- For the purposes of privacy protection, policies and procedures should continue to limit access and analysis of personal information to designated persons and should be subject to record keeping and audit.
- The MPS and related joint policy statement should continue to set out the principles, policies and procedures to be applied to the retention, examination, use and disclosure of personal information, including the manner of destruction or disposal. For transparency purposes, the applicable principles, policies and procedures should be public to the greatest extent possible.

RECOMMENDATION 15

Adopt a coherent framework across the Intelligence and Security Act 2017, a ministerial policy statement and the policies of the Government Communications Security Bureau and the New Zealand Security Intelligence Service's (the Agencies) for the retention and disposal of all information obtained, collected, created and/or managed by the Agencies in the course of exercising their statutory functions, including information that is obtained under an authorisation, as well as by other lawful means. This should include the following elements.

[441] Intelligence and Security Act 2017, s 206(h).

a. Information management policies should apply throughout the intelligence cycle.

b. The necessity and proportionality tests should apply throughout the process of examination, use, retention and disposal of information.

c. Access and analysis of personal information should be limited to designated persons and subject to record keeping and audit requirements.

d. The rules around retention periods for all classes of information should be specified.

e. The manner of destruction or disposal should be specified.

f. The applicable principles, policies and procedures for information retention and disposal should be made public to the greatest extent possible.

CHAPTER 09
Obtaining information from public and private-sector organisations

Introduction

9.1. In this chapter, we address the ways in which Aotearoa New Zealand's two intelligence and security agencies of the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) (the Agencies) access information held by other New Zealand agencies and entities. As the information held by New Zealand agencies and entities contains a high proportion of information on New Zealanders, the legislative framework contains specific safeguards and protections, particularly relating to privacy. (See also chapters 2, 6 and 10.)

9.2. The Intelligence and Security Act 2017 (ISA) sets out four mechanisms through which the Agencies can access this type of information.

- Direct access agreements allow the Agencies to have direct access to databases that store specified public sector information.[442]
- Business records directions authorise the Agencies to request business records from specified private sector businesses, namely banks and telecommunications companies.[443]
- The Agencies can request the voluntary disclosure of information from a wide variety of sources.[444]
- They have access to specified categories of restricted information held by named public sector agencies.[445]

Direct access agreements

9.3. The ISA allows the Agencies to have direct access to certain specified databases provided the access is in accordance with a written Ministerial direct access agreement.[446] This enables one or both Agencies to have direct access to:

- births, deaths, marriages, civil unions and name changes information held by the Registrar-General of Births, Deaths and Marriages

[442] Intelligence and Security Act 2017, ss 124–133.
[443] Sections 143–155.
[444] Sections 120-–122.
[445] Sections 134–142.
[446] Sections 124–133.

- citizenship information held by the Secretary for Internal Affairs
- information collected by the Ministry of Business Innovation and Employment under the Immigration Act 2009
- information collected by the New Zealand Customs Service (Customs) under the Customs and Excise Act 2018
- financial intelligence information held by the New Zealand Police (the Police)
- information held by the Police on people or locations that may pose a physical threat to GCSB or NZSIS employees.[447]

9.4. The Minister responsible for the relevant Agency and the Minister responsible for the agency holding the database (the holder agency) must be satisfied of certain matters before entering into a direct access agreement. These include that direct access is necessary to enable the Agency to perform any of its functions, there are adequate safeguards to protect the privacy of individuals and there are appropriate procedures in place for direct access, use, disclosure and retention of the information.[448]

9.5. Direct access agreements are subject to consultation with the Privacy Commissioner and the Inspector-General of Intelligence and Security (the Inspector-General).[449] The agreement must specify the information that may be accessed, the purpose of the access, the mechanism for access, record keeping, safeguards and storage, retention, disposal and disclosure of the information.[450] It must be published unless there is reason to withhold publication under the Official Information Act 1982 (in which case a summary must be published).[451] The Ministers who have entered into the agreement must review it every three years.[452]

9.6. The Minister responsible for the NZSIS has agreements with:

- the Minister of Customs for the NZSIS to access CusMod information[453]
- the Minister of Internal Affairs for the NZSIS to access birth, death, marriage, civil union and name-change information and citizenship information held by the Secretary for Internal Affairs
- the Minister of Immigration to access the advanced passenger processing (APP) and electronic travel authority (ETA) databases.[454]

9.7. Work is underway to enable the NZSIS to have direct access to financial intelligence information held by the Police. The GCSB has no direct access agreements.

9.8. Four issues have been identified in relation to direct access agreements by the Agencies and submitters.

- The holder agencies and the relevant databases that can be covered by direct access agreements are listed in Schedule 2 of the ISA. This constrains the timely update of the list, and ability to enter into new direct access agreements.

---

447 Schedule 2.
448 Section 126.
449 Sections 127–128.
450 Section 129.
451 Section 131.
452 Sections 132.
453 The database containing customs border crossing information.
454 See, NZSIS "Direct Access Agreements" (nzsis.govt.nz/about-us/working-with-others/).

- There are issues with the scope of the direct access regime, and questions about whether this should be clarified.
- The Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019 (the Royal Commission) recommended a requirement to report on the direct access agreements that have been entered into.
- The Agencies questioned the appropriateness of the three-yearly review period.

Listing holder agencies and databases in Schedule 2 of the ISA

9.9. The direct access agreement provisions were developed in response to the review carried out by Sir Michael Cullen and Dame Patsy Reddy (the Cullen/Reddy review).[455] It recommended that the legislation explicitly permit the Agencies to access and retain certain specified datasets. The 2016 New Zealand Intelligence and Security Bill largely followed the recommended schema, with the holder agencies and specified datasets included in Schedule 2.

9.10. The original intent of the Cullen/Reddy recommendation was to have a reference to the databases included in legislation and to narrow the scope of access through a joint protocol (direct access agreement) agreed between the Minister responsible for the Agencies and the Minister responsible for the holder agency.[456] The review considered that, as the datasets held by other government agencies may contain personal information about a wide range of individuals (the majority of whom would not be of security concern),[457] the Agencies should not be able to see or use all the information the databases contained.[458] Rather, they would be subject to controls set out in the direct access agreements, which would seek to balance the level of interference with individuals' right to privacy against the value of the information to be gained.[459]

9.11. The 2016 Bill provided for Schedule 2 to be amended via an Order in Council.[460] However, submissions were received opposing this, including from the Regulations Review Committee, which sought either the removal of the provision or an amendment to limit it.[461] The New Zealand Law Society submitted that the provision allowing amendment through an Order in Council should be removed on the grounds that it was a "Henry VIII clause"[462] that was not warranted.[463]

9.12. The Agencies have flagged the lack of flexibility to readily amend Schedule 2 because it requires the passage of primary legislation. They suggested that the direct access provisions could be more flexible to allow them to respond to the ever-changing threat environment in a timely way. As a security intelligence agency, the NZSIS has found direct access agreements to be particularly useful and said it would benefit from having a direct access agreement to cover other public

---

[455] Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM *Intelligence and Security in a Free Society – Report of the First Independent Review of Intelligence and Security in New Zealand* (February 2016) (*Cullen/Reddy report*).

[456] Cullen/Reddy report, at [7.16].

[457] Cullen/Reddy report, at [7.7].

[458] Cullen/Reddy report, at [7.15].

[459] Cullen/Reddy report, at [7.16].

[460] An Order in Council is a type of secondary legislation that is made by the Executive Council presided over by the Governor-General of New Zealand.

[461] Regulations Review Committee *Submission on the New Zealand Intelligence and Security Bill* (10 November 2016).

[462] The nature of secondary legislation is that it generally takes effect subject to all primary legislation. It is possible, however, for secondary legislation to amend or override an Act. This requires Parliament to enact an empowering provision expressly authorising secondary legislation with that effect. Empowering provisions of this nature are sometimes called "Henry VIII clauses": Legislation Design and Advisory Committee *Legislation Guidelines* (2021 edition) at [79].

[463] New Zealand Law Society "Submission to the Foreign Affairs, Defence and Trade Select Committee on the New Zealand Intelligence and Security Bill" (11 October 2016) at [5.12].

sector databases, such as the firearms register held by the Police and the National Intelligence Application (NIA) database for information on aliases, known associates and criminal histories. This would go beyond the specified access in Schedule 2 for information from NIA, which is limited to information about people and locations that pose a possible physical threat to GCSB or NZSIS employees, or future access by NZSIS to the firearms register, which will be limited to the purpose of helping determine whether a person is a fit and proper person to possess firearms.[464]

9.13. We have heard from other agencies that the existing direct access agreements are working well and that there is merit in expanding Schedule 2. However, we have also heard that setting up such agreements is resource intensive. Once agreements are established, the Agencies may need specific training on the use of the database and may not have the necessary skills in the subject-matter of the database.

9.14. The core issue is to determine which elements of the direct access to databases should be in primary legislation and which are best left to the direct access agreement. We have reached the following conclusions.

- The ISA should continue to set out the process for entering into direct access agreements.
- Schedule 2 should continue to list the holder agencies with which direct access agreements may be made.
- The databases held by the holder agencies should not be listed in Schedule 2. Rather, they should be dealt with in the direct access agreements themselves.

9.15. Any changes to the process for making direct access agreements or to the Schedule in terms of adding or removing a holder agency would require amendments to the ISA, but changes could be made in relation to datasets simply by agreement between the responsible Ministers.

9.16. The Agencies would still be required to narrow the scope of their access in line with s 126 of the ISA to only that which is necessary to enable them to perform their functions and to ensure that adequate safeguards are in place.

9.17. Additionally, there would still be a requirement for the Ministers responsible for the Agency and the holder agency to agree on access to the database[465] and a requirement that the agreement be published, either as a new access agreement or as a variation to an existing one.[466] This means that transparency over which databases the Agencies have access to, for what purposes and on what terms would be maintained.

9.18. This approach means Parliament would continue to determine which public sector agencies may enter into direct access agreements with the Agencies and allow public participation in the process via submissions to select committee. However, the specifics of the agreements would be decided by the executive, in the form of the Minister responsible for the Agencies and the Minister responsible for the holder agency. This would be consistent with New Zealand's usual approach to legislation, with broad policy intent outlined in the Act and detail in the regulations.

9.19. The original intent of the Cullen/Reddy recommendation was not to identify the databases and agencies holding the databases in the Schedule but to narrow the scope of access through the direct access agreements. This proposed solution is consistent with this original intent but removes one level of detail from the Schedule (ie, the database).

---

[464] See s 107 of the Arms Legislation Act 2020, which according to s 2(5) is not yet in effect.

[465] Intelligence and Security Act 2017, s 125.

[466] Section 131.

The scope of the direct access regime and publicly available information

9.20. The direct access regime in subpart 2 of Part 5 of the ISA relates only to "specified public sector information" (which is not defined) and proceeds to identify specific public-sector bodies in Schedule 2 and the information that may be obtained from these bodies. There are other databases storing information in New Zealand that are not specified in Schedule 2. We provide two examples.

- The MotoChek database of Motor Vehicle Register information held by Waka Kotahi (New Zealand Transport Agency) may be accessed by authorised users in bulk or on a frequent and ongoing basis.[467] It would be expected that an Agency would [most likely] have some form of access to MotoChek.
- It has been acknowledged that the NZSIS has access to most CCTV cameras in a New Zealand city centre,[468] and this access is governed by a memorandum of understanding between the NZSIS and the chief executive of the CCTV provider.[469] The Inspector-General recommended that advice be sought from the Solicitor-General on the legal basis for accessing CCTV footage.[470]

9.21. These two examples illustrate that there is a lack of clarity over the scope of the direct access regime. Neither database is, strictly speaking, a public-sector database. Therefore, neither would be covered by amendments to Schedule 2 (although it is possible that they could be captured in this way).

9.22. Also, because the ISA only applies to specified public-sector agencies, it does not address the potential for direct access to other databases held by non-public-sector agencies, including publicly accessible or commercially available databases. Some of these databases only contain publicly available information where the individuals concerned would not have any reasonable expectation of privacy (such as online telephone directories for businesses and residences). However, others may contain personal information in which there may be a reasonable expectation of privacy.

9.23. With regard to the latter, there is a balance to be struck between the usefulness of the Agencies having direct access to New Zealand databases to fulfil their functions, and privacy interests in the personal information contained in the databases. Given the secrecy of the intelligence function and the potential intrusion on the privacy of individuals, there is a case for controls on the extent to which the Agencies can have direct access to databases that contain personal information in respect of which the individuals concerned have a reasonable expectation of privacy. We have not reviewed the various databases, not held by the specified public-sector agencies, that are publicly or commercially available or available with consent nor whether it would be necessary and proportionate for the Agencies to have access to such databases to enable them to fulfil their functions.

---

[467] Waka Kotahi "Who can access Motor Vehicle Register Information" (nzta.govt.nz/vehicles/how-the-motor-vehicle-register-affects-you/).

[468] Inspector-General of Intelligence and Security *Review of NZSIS use of closed circuit television (CCTV)* (online, June 2021) at [11].

[469] Above n, at [37].

[470] Above n, at [36] and recommendation 3 at [38].

9.24. Should the Agencies wish to pursue this, further policy work would be needed to understand the appropriateness of the Agencies having direct access to such databases and whether such databases should come under the umbrella of a broader direct access agreements regime or another form of authorisation.

9.25. At a minimum, we believe such access should be subject to specified, written agreements with the database holder, with the agreements entered into following consultation with the Privacy Commissioner and Inspector-General and meeting transparency and reporting requirements. Such controls are necessary in order to address the privacy interests in personal information contained in the databases.

Reporting on direct access agreements

9.26. The Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019 noted that the NZSIS had only entered into a limited number of the types of direct access agreements that are permitted under the ISA.[471] The Royal Commission felt there were no mechanisms to encourage other agencies to enter into these agreements and adding a statutory requirement to report on progress might help speed up the finalisation of the agreements.[472]

9.27. There are a range of reasons why direct access agreements have not been entered into, including the resources required to negotiate them, technical difficulties arising from direct access and costs. Although direct access agreements provide valuable information, they are not the only way the Agencies can seek database information. In particular, the voluntary sharing provisions of the ISA allow information to be obtained on a case-by-case basis from New Zealand public-sector, quasi-public-sector and private-sector agencies. Thus, a reporting requirement, while useful for transparency, may not achieve the Royal Commission's aim.

Reviewing direct access agreements every three years

9.28. The direct access agreements must be reviewed every three years. This provides a mechanism to determine whether an agreement should continue and whether any changes are needed. It also provides an opportunity for the respective Ministers to review the effectiveness of the agreement and for the Agencies to consult the Privacy Commissioner and the Inspector-General. The Agencies have suggested the review period be extended from 3 to 5 years. Their justification is largely based on resource requirements to review the agreements. This does not seem a sufficiently strong justification to amend the ISA. We have found no other reasons to suggest the 3-year period is inappropriate.

9.29. The Inspector-General has raised an issue concerning the length of time it takes to review and approve direct access agreements.[473] The review of the agreements and approval of any amendments is not wholly within the Agencies' control. To encourage timely completion of the reviews, we suggest the Minister responsible for the Agency and the Minister responsible for the holding agency should submit a joint report to the Intelligence and Security Committee to confirm that the direct access agreement remains fit for purpose or advise of any changes to the agreement, within 12 months of the review commencing.

---

471 *Royal Commission of Inquiry Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) at part 8, chapter 14 at [89] (Royal Commission report).

472 Royal Commission report, at part 8, chapter 14 [91].

473 Inspector-General of Intelligence and Security *Annual Report for the year 1 July 2021 to 30 June 2022* (online, November 2022) at 6-7.

RECOMMENDATION 16

With respect to the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) (the Agencies) having direct access to database information held by other public sector agencies

a. Amend Schedule 2 (Databases accessible to the Agencies) of the Intelligence and Security Act 2017 to remove the list of databases accessible to the Agencies, but retain the names of the holder agencies (eg, New Zealand Police, New Zealand Customs Service) with which either the GCSB or the NZSIS may enter into direct access agreements.

b. The Government should consider undertaking further policy work on the appropriateness of the Agencies having direct access to non-public sector agency databases containing information in respect of which there may be a reasonable expectation of privacy, and if so, whether such access should come under the umbrella of a broader direct access agreements regime or another form of authorisation. Any such access should be subject to specified and written agreements with the database holder, which would be reviewed by the Privacy Commissioner and Inspector-General and subject to transparency and reporting requirements.

c. The Government should consider requiring the Minister responsible for the Agency and the Minister responsible for the holding agency to submit a joint report to the Intelligence and Security Committee within 12 months of the review of a direct access agreement commencing.

Business records directions

9.30. Under Subpart 4 of Part 5 of the ISA, the Directors-General of the Agencies may apply to the responsible Minister and to the Chief Commissioner of Intelligence Warrants for approval to obtain business records from a specified business agency (ie, telecommunication network operators and financial service providers).[474] Once an application is approved, the agencies may request business records from that business agency for the duration of the approval (maximum 6 months, which in appendix C we recommend increasing to 12 months) and in line with the circumstances agreed under the approval. This may include restrictions or conditions on the information that can be collected under the business records direction.[475]

9.31. Business records are defined in s 144 of the ISA and include such information as customer and subscriber names and contact details, bank account and credit card details, IP addresses, billing information and records, call associated data, device-related information, mobile data usage, information on linked accounts and details of people communicating with the network operator. Business records do not include such things as the content of communications or web browsing histories, for which the Agencies would require a warrant. Information regarding the service provider's employees and the business operations of the provider are also excluded.[476]

474 Intelligence and Security Act 2017, s 145.
475 Section 147.
476 Section 144.

9.32. During the select committee process for the 2016 New Zealand Intelligence and Security Bill, the New Zealand Bankers Association and several telecommunication companies made submissions outlining that receiving the Agencies' requests for voluntary disclosure puts them in a difficult position between providing assistance that may be in the public interest and their duties of confidence and privacy to their customers.[477] They requested they be compelled to provide information to the Agencies, as opposed to providing the information on a voluntary basis.[478] This request resulted in the current business records directions regime.[479]

Expanding the definition of business agencies

9.33. Currently, the ISA restricts the application of business records directions to telecommunications network operators and financial service providers.[480] Should the Agencies wish to request business records from another type of public- or private-sector agency, they would have to seek voluntary disclosures[481] or a warrant. Section 121 allows the Agencies to request information from any other agency (ie, any person in the public or private sector, including departments) on a voluntary basis. It does not require or compel the person receiving the request to provide the information to the Agency.

9.34. It has been proposed that business agencies outside telecommunications network operators and financial service providers also struggle to balance the privacy and confidence of their customers with assisting the Agencies in protecting New Zealand's national security. Requesting information to be voluntarily disclosed under s 121 is likely to place an individual business in the unenviable position of having to weigh their internal privacy policies and current risk appetite against the potential national security implications of not disclosing the information.

9.35. It is likely other business agencies would prefer to be compelled to provide information to the Agencies under the business records directions regime, as opposed to providing the information voluntarily. However, it would be unjustifiably broad to make all businesses subject to compulsion under the ISA, without requiring the Agencies to obtain a warrant.

9.36. Although we consider it may be appropriate to expand the definition of business agencies under the ISA, most likely to include airline and perhaps other transportation operators and an expanded range of communications providers, further policy work would be required to ensure that any expansion of powers under the business records directions regime is appropriately balanced with the right to privacy and other considerations. While some businesses may prefer to be subject to a business records direction, we have not received sufficient information to draw any conclusions on which businesses these might be. We therefore recommend the government undertake policy work on whether the business records directions regime should be extended to other business agencies, including consultation with the potentially affected businesses and the wider public, before proposing any change to the scope of business records directions.

---

477 New Zealand Bankers Association "Submission to the Foreign Affairs, Defence and Trade Select Committee on the New Zealand Intelligence and Security Bill" (7 October 2016) at [10].

478 New Zealand Bankers Association "Submission to the Foreign Affairs, Defence and Trade Select Committee on the New Zealand Intelligence and Security Bill" (7 October 2016); Two Degrees Mobile Limited "Submission on the New Zealand Intelligence and Security Bill" (7 October 2016); Spark "Submission: New Zealand Intelligence and Security Bill" (7 October 2016); Vodafone New Zealand "Submission on the New Zealand Intelligence and Security Bill" (7 October 2016).

479 Intelligence and Security Act 2017, ss 143–155.

480 Section 144.

481 Sections 121 and 122.

RECOMMENDATION 17

The Government should undertake policy work to determine whether the business records directions regime, which enables the Government Communications Security Bureau and the New Zealand Security Intelligence Service to obtain business records from telecommunications network operators and financial service providers, should be extended to other business agencies, and this should include consultation with the potentially affected businesses and the wider public.

Requests and disclosures of information

9.37. Section 121 of the ISA recognises the Agencies' ability to request information from any person or department on a voluntary basis if the relevant Agency Director-General believes the information is necessary to enable the Agency to perform any of its functions.

> **Requests for information**
>
> (1) The Director-General of an intelligence and security agency may request information from any other agency if the Director-General believes on reasonable grounds that the information is necessary to enable the intelligence and security agency to perform any of its functions.
>
> (2) A request must—
>
> (a) provide details of the information requested; and
>
> (b) confirm that the information is necessary to enable the intelligence and security agency to perform any of its functions.

9.38. Section 122 recognises the existing ability of a person or department to disclose information to an Agency if they believe disclosure is necessary to enable the Agency to perform its functions. Disclosure may be made by the person either on their own initiative or at the request of Agency. The provision does not require, or compel, the person to provide the information.[482] Rather it is voluntarily provided on a case-by-case basis.

9.39. During the development of the ISA, it was acknowledged that it was not strictly necessary to include these provisions in the legislation as there is nothing preventing the Agencies requesting information, nor other parties disclosing information to the Agencies in the absence of other constraints. However, the provisions were included for two key reasons. These are:[483]

- to provide transparency around the Agencies' access to information
- to address the risk that the courts would determine that the Agencies cannot ask for information if that is not specifically provided for in the legislation.

9.40. In general, we believe the provisions for the request and disclosure of information are working as intended. The Agencies have suggested the definition of agency in s 118 be amended to make it clear that it includes foreign public agencies. However, we are not persuaded that Part 5 was

[482] Section 120(b).

[483] Department of the Prime Minister and Cabinet *New Zealand Intelligence and Security Bill, Departmental Report to the Foreign Affairs, Defence and Trade Committee* (December 2016) at [744] and [746].

intended to apply to foreign public agencies and do not consider that a case has been made justifying an extension.

9.41. Section 4 of the ISA includes two relevant definitions. First, it defines foreign public agency. Second, it defines "public authority" in a way that includes both New Zealand and foreign public agencies. Accordingly, when the ISA uses the term "public authority", as it does in numerous sections, it will include foreign public authorities unless there is a specific exception. Part 5, which relates to "accessing information held by other agencies" has a definition of agency that is general but does not specifically include foreign public agencies. Given the context of the ISA as a whole, and the particular context of Part 5, we consider that the word "agency" in Part 5 does not include foreign agencies.

9.42. Moreover, in our view, the Agencies' proposed amendment would not fit well with the scheme of Part 5. We note that the Agencies have advised us they can continue to request information from foreign public agencies by relying on common law and the cooperation functions described at s 10(2) and 11(2) of the ISA. We express no view about that.

9.43. We are not suggesting any significant changes to these provisions, but several routine improvements are addressed in appendix C of this report.

Access to restricted information

9.44. As explained above, the Agencies can request information be disclosed from another government agency under s 121 of the ISA. Other agencies may also share information with the Agencies under information privacy principle 11 of the Privacy Act 2020, which allows for the disclosure of information if the agency believes, on reasonable grounds, that the disclosure of that information is necessary to enable an intelligence and security agency to perform any of its functions.[484] However, in some instances, an agency may be prevented from providing the information due to legislation that restricts its disclosure.

9.45. The Cullen/Reddy review noted that the Agencies may need to access this restricted information on a case-by-case basis.[485] The report recommended allowing the Agencies to access this information if it was necessary to perform a statutory function and was proportionate to the objective being achieved – in line with Cullen/Reddy's proposed warranting regime. [486]

9.46. The Cullen/Reddy recommendation is reflected in the ISA, which allows the Agencies to apply to the Minister responsible for the Agencies and, in the case of information on New Zealanders, to the Chief Commissioner of Intelligence Warrants to access restricted information.[487]

9.47. The ISA specifies the type of restricted information the Agencies can access on a case-by-case basis,[488] including:

- information that a revenue officer must keep confidential under s 18(1) of the Tax Administration Act 1994

[484] Privacy Act 2020, s 22, Information privacy principle 11.
[485] Cullen/Reddy report, at [7.11].
[486] Cullen/Reddy report, at [7.22].
[487] Intelligence and Security Act 2017, s 136.
[488] Section 135.

- information relating to national student numbers assigned by the Secretary for Education under Schedule 3 of the Education and Training Act 2020 to students enrolled with a tertiary education provider;
- information relating to an adoption held by the Registrar-General under section 19(1) of the Births, Deaths, Marriages, and Relationships Registration Act 1995
- photographic images used for driver licences that are stored under section 28(5) of the Land Transport Act 1998.

9.48. Four issues have arisen in relation to the restricted information regime. These relate to:

- the scope of the restricted information regime as it pertains to information relating to New Zealanders
- whether the definition of restricted information covers all the information the Agencies may require access to in order to fulfil their functions
- the relationship between the restricted information regime and the warranting regime
- whether government agencies should have the power to provide information to the Agencies that is restricted by other legislation where this is necessary for national security purposes.

Scope of the restricted information regime

9.49. The restricted information regime operates differently for New Zealanders and non-New Zealanders. In the case of information on New Zealanders, a Commissioner of Intelligence Warrants as well as the Minister responsible for the Agency must grant permission to access restricted information, and they must have reasonable grounds to suspect that the person concerned is acting or purporting to act, for or on behalf of a foreign person, foreign organisation or a designated terrorist entity.[489]

9.50. Although we have recommended removing the Type 1 / Type 2 distinction from warranting for national security purposes, we have also recommended retaining the distinction between New Zealanders and non-New Zealanders in relation to collecting intelligence for the purposes of international relations and well-being and economic well-being. This distinction is based on the criteria colloquially referred to as 'agent of a foreign power'. This is the same criteria used in determining access to restricted information of New Zealanders.

9.51. We therefore do not recommend broadening the scope of access to restricted information for New Zealanders and recommend retaining ss 136–138.

Definition of restricted information

9.52. The ISA allows the Agencies to apply for access to a defined category of restricted information. However, during the course of our review, it was brought to our attention that s 135 is not a definitive list of information that other public agencies are prevented from sharing with the Agencies by applicable legislation. For example, Inland Revenue submitted that the current definition of 'restricted information' in s 135 applies only to "sensitive revenue information"

[489] Section 137.

whereas Inland Revenue also holds "revenue information", the unauthorised disclosure of which is subject to criminal penalites.[490]

9.53. We have not undertaken a comprehensive review of the different kinds of restricted information that it may be necessary and proportionate for the Agencies to access in order to perform their functions. The Inland Review example shows there may be other information that may appropriately be brought within the restricted information regime in the ISA. We therefore recommend the Department of the Prime Minister and Cabinet work with the Agencies, and other government agencies, to determine whether any further information should be brought within the restricted information regime of the ISA.

Restricted information regime and the warranting regime

9.54. The Cullen/Reddy review recommended that approvals for access to restricted information parallel warrants and access be considered on a case-by-case basis.[491] This ensures that access is only granted when the necessity and proportionality of obtaining the information is considered within the operational context of the application for access.

9.55. The Agencies suggested that access to restricted information be included as a power within the warranting framework. However, making access to restricted information a separate application to a warrant ensures the Agencies will limit their applications for restricted information to the situations where a clear case can be made for the operational benefit of obtaining the specified information and where it is clear the information could not be obtained via less intrusive means. We recommend retaining the distinction between warranted activities and access to restricted information.

Proactive information sharing by other government agencies for national security purposes

9.56. Other government agencies have raised the issue that, on occasion, they may come across information that is relevant to national security, but they are prevented from sharing that information with the Agencies by their own governing legislation. This is mentioned further in chapter 10 on information sharing but also arises in relation to obtaining information from public agencies.

- For example, Inland Revenue is prevented from sharing information with the Agencies because the permitted disclosures provisions of ss 18D to 18J of the Tax Administration Act 1994 make no provision for this.
- In other instances, these agencies are able to share information that is otherwise prohibited from disclosure, such as to the Police for anti-money laundering or countering the financing of terrorism purposes.[492]

9.57. It seems sensible to allow an agency that holds information that it is otherwise prohibited from disclosing under its legislation to share information with the Agencies if the agency believes, on reasonable grounds, that the disclosure of the information is necessary or desirable for the

[490] See s 16C(2), 18(3) and 143C(1)(b) of the Tax Administration Act 1994.
[491] Cullen/Reddy report, at [7.21]–[7.22].
[492] Anti-Money Laundering and Countering Financing of Terrorism Act 2009, s 140.

maintenance of New Zealand's national security. However, this is likely to require amendments to the governing legislation of these agencies. There would therefore need to be consultation with the government agencies concerned, including on necessary amendments to their legislation.[493]

9.58. An alternative might be to handle access to certain restricted information, such as tax information, in a similar manner to the approved information sharing agreements negotiated between government agencies under Schedule 2 to the Privacy Act 2020. However, this seems to parallel the restricted information regime established in the ISA, and there is therefore some question of the usefulness of such an approach.

9.59. The inclusion of a proposal to permit disclosure of information that is otherwise not able to be shared would need oversight and monitoring by the Privacy Commissioner and Inspector-General to ensure it is only used in the circumstances prescribed and does not become a catch-all for the general sharing of information to which legislative disclosure prohibitions apply.

9.60. We acknowledge this raises complex issues. For this reason, our recommendation only extends to **considering** such a permitted disclosure regime.

RECOMMENDATION 18

With respect to accessing restricted information that is specified in the Intelligence and Security Act 2017 (ISA) as information to which access is restricted by another statute:

a. The Department of the Prime Minister and Cabinet should work with the Government Communications Security Bureau and the New Zealand Security Intelligence Service (the Agencies), and other Government agencies, to determine whether any further information should be brought within the restricted information regime of the ISA.

b. The Government should consider amending the ISA to enable other domestic agencies to proactively share information they are otherwise prevented by statute from sharing with the Agencies if they believe on reasonable grounds that the disclosure of that information is necessary or desirable for the maintenance of New Zealand's national security and provided the disclosure is subject to appropriate controls.

[493] For example, the proposed solution for Inland Revenue will require an amendment to the Tax Administration Act 1994 to include an additional 'permitted disclosure' that would enable Inland Revenue to make a proactive disclosure.

SECTION 04

Sharing and assessment of information

CHAPTER 10
Inter-agency cooperation and information sharing

Introduction

10.1. Any information collected by the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) (the Agencies) must be analysed and assessed and then shared in order to provide benefit to the government in contributing to the protection of national security, the international relations and well-being of Aotearoa New Zealand or the country's economic well-being.

10.2. Under the Intelligence and Security Act 2017 (ISA), intelligence is shared under both the Agencies' intelligence collection and analysis function as well as their protective security functions. In chapter 3, we raised the importance of coherence and coordination between the intelligence functions of relevant domestic agencies. This is particularly relevant to the sharing of intelligence so that it can be used by domestic agencies to respond to national security threats or criminal activity. We also discussed New Zealand's participation in the Five Eyes relationship, which allows New Zealand to exchange information with its foreign partners in the relationship.[494]

10.3. The terms of reference for this review require us to consider how the ISA may best enable the Agencies to "appropriately and effectively cooperate and share information with New Zealand government agencies and other partners".[495]

10.4. We start by addressing cooperation, advice and assistance with the New Zealand Police (the Police) and the New Zealand Defence Force (NZDF) under the ISA. This covers cooperation under s 13 of the ISA to facilitate the performance of the functions of these agencies and cooperation under s 14 to respond to an imminent threat. We also consider assistance to give effect to an authorisation under s 51 of the ISA.

10.5. We then turn to the sharing of intelligence and analysis with domestic agencies and with overseas partners and consider the controls on intelligence sharing.

Cooperation, advice and assistance

10.6. Under the ISA, the Agencies may provide cooperation, advice and assistance to other public agencies in several contexts. First, they may do so in performing their function under s 10(1) in

---

494 An intelligence partnership between Australia, Canada, New Zealand, the United Kingdom and the United States of America.

495 Appendix A, at [2.5].

collecting and analysing intelligence[496] or in performing their function under s 11(1) of providing protective security services, advice and assistance.[497] Second, the agencies have a function of cooperation under s 13(1) between themselves and with the NZDF and the Police. Third, they have a function under s 14 of cooperation, advice and assistance with others in responding to an imminent threat to the life or safety of a New Zealander or others under certain circumstances.

10.7. The genesis of the cooperation, advice and assistance functions of the Agencies can be traced to the Government Communications Security Bureau Act 2003 (the GCSB Act), which provided the GCSB with a broad cooperation, advice and assistance function, including on any matter relevant to the functions of another public authority or entity. Following the issues with the surveillance of Mr Kim Dotcom, the GCSB initially halted providing cooperation, advice and assistance to public agencies due to uncertainty about the statutory basis for doing so.[498] The GCSB Act was amended in 2013 to clarify the GCSB's functions relating to cooperation, advice and assistance with other agencies in New Zealand and, in particular, to provide limits and oversight for GCSB when it exercised this function. To strengthen the accountability provisions and improve transparency, an annual reporting requirement on the cooperation, advice and assistance function was introduced by Hon Peter Dunne at the Committee of the Whole House stage[499] and passed into law.

10.8. By 2016, the review carried out by Sir Michael Cullen and Dame Patsy Reddy (the Cullen/Reddy review)[500] had a different concern – namely that the Agencies were not cooperating with each other or with the rest of the public sector sufficiently to protect New Zealand's national security.[501]

> … a recurring theme throughout our review has been the need for the Agencies to work together and with the broader public sector more effectively. In the modern technological and threat environment, the Agencies will be of little use if they cannot do this. Information from human or electronic sources will usually only provide pieces of a puzzle; they must be combined to provide a full picture. We therefore encourage the Agencies to develop a closer working relationship. While this process has already begun since the co-location of the Agencies, we consider there is much greater scope for cooperation.

10.9. The Cullen/Reddy review recommended that one of the common functions of GCSB and NZSIS be cooperating with and assisting other specified government agencies, including the Police and the NZDF, to carry out their functions in accordance with their governing legislation.[502]

> In our view, it would be preferable for the legislation to provide explicitly for the NZSIS to assist Police, NZDF and the GCSB in the performance of those agencies' functions. These agencies (in particular the NZSIS and Police due to their close working relationship and the importance of separating intelligence collection from enforcement), should develop joint operating protocols governing how they work together.

---

496 Intelligence and Security Act 2017, s 10(2).

497 Section 11(2)–(3).

498 For further details, see Rebecca Kitteridge *Review of Compliance at the Government Communications Security Bureau* (March 2013).

499 Supplementary Order Paper 2013 (308) Government Communications Security Bureau and Related Legislation Amendment Bill (109-2).

500 Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM *Intelligence and Security in a Free Society – Report of the First Independent Review of Intelligence and Security in New Zealand* (February 2016) (*Cullen/Reddy report*).

501 Cullen/Reddy report, concluding remarks at 146.

502 Cullen/Reddy report, at [5.57].

10.10. In addition, the Cullen/Reddy review recommended the Agencies, as a matter of practice, develop joint operating protocols with other agencies. Sections 13 and 14 of the ISA were enacted against this background. They were not the subject of Parliamentary debate during the enactment of the ISA.

Constraints on advice and assistance to Police and NZDF

10.11. For present purposes, s 13(1) of the ISA is the more significant of the two provisions. It provides:

> **Co-operation with other public authorities to facilitate their functions**
>
> (1) It is a function of the intelligence and security Agencies to—
>
> (a) co-operate with—
>
> (i) each other; and
>
> (ii) the New Zealand Police; and
>
> (iii) the New Zealand Defence Force; and
>
> (b) provide advice and assistance to the New Zealand Police and the New Zealand Defence Force for the purpose of facilitating the performance or exercise of the functions, duties, or powers of those public authorities.

10.12. This provision almost wholly replicates s 8C of the Government Communications Security Bureau Amendment Act 2013. As can be seen, however, although the section heading refers to "co-operation", s 13(1) differentiates in paragraphs (a) and (b) between "co-operation with" and providing "advice and assistance to" the Police and the NZDF. This distinction was the only change to the provision and is significant because the section emphasises the importance of cooperation while retaining greater constraints on the provision of advice and assistance to the Police and the NZDF to facilitate the exercise of the functions of those public authorities.

10.13. In particular, s 13 places parameters around the provision of "advice and assistance" under s 13(1)(b) to ensure it relates to activities that the Police or the NZDF may lawfully carry out in the performance of their functions. Section 13(2) states:

> (2) An intelligence and security agency may perform the function under subsection (1)(b)—
>
> (a) only to the extent that the advice and assistance are provided for the purpose of activities that the public authority may lawfully carry out; and
>
> (b) subject to and in accordance with any limitations, restrictions, and protections under which those public authorities perform or exercise their functions, duties, and powers; and
>
> (c) even though the advice and assistance might involve the exercise of powers or the sharing of capabilities that the intelligence and security agency is not, or could not be, authorised to exercise or share in the performance of its other functions.

10.14. In addition, s 13(3) provides that, when giving advice and assistance to either the Police or the NZDF, the relevant Agency will be subject to the same jurisdictional oversight arrangements as apply to the Police or the NZDF, as the case may be, as well as to the jurisdiction of the Inspector-General of Intelligence and Security (the Inspector-General). In the case of the Police, for example, this means the relevant Agency will be subject to the oversight of the Independent

Police Conduct Authority, as well as that of the Inspector-General. The same situation would apply in relation to the NZDF if the government proceeds with the current proposal to establish an Inspector-General of Defence.

10.15. There are two further important points:

- The Agencies are required to provide information on the number of occasions they have provided "advice and assistance" to the Police and the NZDF under s 13(1)(b) in their annual reports.[503] There is no such reporting requirement in relation to "cooperation" under s 13(1)(a).
- One of the exceptions to the limitation that it is not a function of an Agency to enforce measures for national security is where the Agency is performing a function under s 13.[504]

Annual reporting of advice and assistance to NZDF and Police under the ISA

10.16. Since the Act came into force, the NZSIS has only reported four instances of providing advice and assistance under s 13(1)(b). It is not clear whether this assistance was rendered to the Police or the NZDF.[505] GCSB has reported two instances – once to the NZDF and once to the Police.[506]

10.17. Although this reporting suggests that the Agencies have provided limited assistance to the Police and the NZDF to facilitate the performance of their functions, elsewhere in their public documents, the Agencies state that they work closely with both the Police and the NZDF. We give the following three examples.

- In its 2020 annual report, the NZSIS noted that its functions include:[507]

  > Cooperating with the GCSB, the NZDF and New Zealand Police *to facilitate the performance of their functions*. (Emphasis added.)

  Later in the report, the NZSIS referred to its domestic partnerships, describing Police as a "key partner".[508] The report then said:

  > NZSIS provides assistance and advice to these agencies in matters relating to national security and assists with the protection of New Zealanders overseas. This entails contributing to relevant cross-agency Cabinet decisions, conducting joint operational work, *sharing specialist capabilities to ensure other agencies can perform their roles and functions*, and undertaking joint operational initiatives. (Emphasis added.)

- In its strategy for the period 2018–2022, the GCSB said it would fulfil its objectives by providing:[509]

---

503 Intelligence and Security Act 2017, s 221(2)(a). The reporting requirement was introduced into the previous statutory regime at the instigation of Hon Peter Dunne in the same supplementary order paper that introduced periodic reviews.

504 Section 16(b).

505 New Zealand Security Intelligence Service *2020 Annual Report* (online, 2020) at 51; New Zealand Security Intelligence Service *2021 Annual Report* (online, 2021) at 73.

506 Government Communications Security Bureau *2018 Annual Report* (online, 2018) at 11.

507 New Zealand Security Intelligence Service *2020 Annual Report* (online, 2020) at 9.

508 Above n, at 49.

509 Government Communications Security Bureau, *GCSB Strategy 2018*-2022, 3 August 2018, released under the Official Information Act 1982 at 3.

> Specialist assistance to the New Zealand Security and Intelligence Service (NZSIS), the New Zealand Defence Force (NZDF) and the New Zealand Police (NZP) *in the performance of their functions*. (Emphasis added.)

- In its annual report for 2020, the GCSB stated:[510]

> The GCSB responds to requests for intelligence from, and provides technical assistance to, the NZSIS and New Zealand Police on request. Further, the GCSB has contributed to development of the Police-led Transnational Organised Crime Strategy.

10.18. Our observations during the review confirm there are areas where there is close cooperation between the Agencies and the NZDF and/or the Police. We assumed the Agencies would be reporting significant provision of advice and assistance to the Police and the NZDF to facilitate the performance of their functions under s 13(1)(b). In fact, the reporting indicates the Agencies have provided very little advice and assistance under s 13(1)(b). This raises the question whether some of what the Agencies might describe as "cooperation" should have been reported as "advice and assistance" under s 13(1)(b).

10.19. We have discussed this with the Agencies. In our view, they have adopted an approach to the interpretation of s 13(1)(b) that is narrower than the language, properly interpreted, requires. In essence, the Agencies' position is that they only report "advice and assistance" under s 13(1)(b) when they are 'standing in the shoes' of the Police or the NZDF, for example, when they are helping the Police under a police warrant or otherwise acting effectively as Police (or NZDF) personnel.

10.20. However, the language of s 13(1)(b) is broader than that. It refers to providing advice and assistance to the Police or the NZDF "for the purpose of **facilitating** the performance or exercise of the functions, duties, or powers of those public authorities". "Facilitating" means to make easier or assist. We do not see this as limited to 'standing in the shoes' of the relevant organisation.

10.21. To give a hypothetical example, if the Police decided to send several officers on an overseas deployment as part of an international policing group and the NZSIS gave the officers some specialist training before the deployment to enhance their ability to perform their roles during the deployment, that would generally constitute advice or assistance under s 13(1)(b), even though the NZSIS would not be standing in the shoes of the Police.

10.22. We interpret the various provisions about cooperation, advice and assistance as follows.

- When performing a function under ss 10 or 11, an Agency may cooperate with, or provide advice and assistance to, among others, the Police and the NZDF.
- Under s 13(1)(b), an Agency may provide "advice and assistance" to the Police or the NZDF to help them perform their functions. Taking the Police as an example, where an Agency provides advice or assistance to the Police for the purpose of enabling the Police to fulfil their law enforcement function (for example, by assisting the Police to access a computer system under a Police warrant), the Agency must be acting under s13(1)(b). This attracts the reporting obligation.
- Under s 13(1)(a), the Agencies have a function of cooperating with each other and with the Police and the NZDF. The word 'cooperate' means to work together toward a common goal; it can also mean to assist someone or comply with their requests. The latter meaning

[510] Government Communications Security Bureau *2020 Annual Report* (online, 2020) at 29.

would include "advice or assistance", but, if 'cooperate' were given that meaning, s 13(1)(a) would conflict with s 13(1)(b) and the regime it establishes.

- If "cooperate" in s 13(1)(a) is given the former meaning (working together toward a common goal), the relationship between s 13(1)(a) and 13(1)(b) becomes clear. The functions of an Agency and the Police will sometimes overlap, in the sense that both have national security functions, and those of the Police are not limited to law enforcement but include activities such as threat discovery and prevention. As a consequence, the Agency and the Police can cooperate, in the sense of work together towards a common goal, while both are performing their functions. However, once the activities of the Police are properly characterised as law enforcement, the Agency providing assistance would be moving outside its functions and could not utilise s 13(1)(a) but would have to act under s 13(1)(b). We consider that this approach accords with the legislative origins of the reporting requirement and the Agencies should be reporting consistently with it.

10.23. This interpretation creates a difficulty, however. Where the NZSIS and the Police are co-located and operate jointly in relation to, say, counterterrorism, it can often be difficult to draw lines between functions as clearly as the sections contemplate. In that joint operating environment, where the NZSIS and the Police are working together on counterterrorism issues, both will undertake intelligence-gathering activities, but the Police will almost inevitably also perform law enforcement functions some of the time. It may be unrealistic in that situation to require the NZSIS to distinguish, for reporting purposes, between joint intelligence-gathering activities and activities that assist the Police in their law enforcement functions.

10.24. Accordingly, while we agree with the concerns that led to the current legislative structure, we consider it needs some modification to take account of legitimate joint-operational arrangements. We have not been able to develop an alternative approach in the time available but recommend that consideration be given to making explicit allowance for joint-operational activities of the type described.

RECOMMENDATION 19

The Government should consider amending section 13 (Cooperation with other public authorities to facilitate their functions) of the Intelligence and Security Act 2017 to clarify the scope of "cooperation" under section 13(1)(a) and the provision of "advice and assistance" under section 13(1)(b) and how this distinction operates in the context of joint operations.

Cooperation to respond to an imminent threat

10.25. Section 14 of the ISA enables the Agencies to cooperate with, and provide advice and assistance to, others to respond to an imminent threat to the life or safety of a New Zealander or others under designated circumstances. Specifically, the section provides:

> **Co-operation with other entities to respond to imminent threat**
>
> (1) It is a function of the intelligence and security agencies to co-operate with, and provide advice and assistance to, a person, class of persons, or public authority

> (whether in New Zealand or overseas) that is responding to an imminent threat to the life or safety of—
>
> (a) any person in New Zealand; or
>
> (b) any New Zealand citizen who is overseas; or
>
> (c) any permanent resident of New Zealand who is overseas; or
>
> (d) any person in an area in respect of which New Zealand has search and rescue responsibilities under international law; or
>
> (e) any person outside the territorial jurisdiction of any country.

10.26. The concept of "imminent threat" (including "imminence" and what threat activities fall under s 14) is unclear to some agencies. They are also unsure what conditions need to exist before other agencies can receive support from the Agencies under s 14.

10.27. The regulatory impact statement on the policy of the New Zealand Intelligence and Security Bill 2016 identified that, previously, no legislative provision existed that allowed either Agency to support organisations such as Maritime New Zealand or the Royal New Zealand Coastguard to assist with a search and rescue of, for example, a missing tramper or lost yacht (eg, by providing information obtained from intercepting communications).[511]

10.28. Collecting and providing such information to relevant entities appears to align with the government's broad "ensuring public safety" objective of its 'all hazards, all risks' approach to national security[512] and the Agencies' function of collecting and analysing intelligence and cooperating with and providing advice and assistance to any person or class of persons approved by the responsible Minister, or public authorities.[513] However, it does not appear to align with the required criteria to obtain a type 1 intelligence warrant against a New Zealander, which includes protecting national security and addressing specified harms (eg, terrorism or violent extremism, espionage or foreign interference, sabotage, serious crime, threats to information and information infrastructure, international security and New Zealand sovereignty).[514]

10.29. In this context, information can be collected on a New Zealander to protect against imminent traditional threats to national security, but there may be situations when this is not possible for wider imminent threats, such as those posed to individual safety from environmental or non-traditional threats. Section 14 appears to fill this gap.

10.30. Protections are also in place to ensure the function is not used in a way that goes beyond what the Agencies might otherwise be empowered to do. Specifically, s 14(2) states:

> (2) An intelligence and security agency may perform this function—
>
> (a) only to the extent that the co-operation, advice, and assistance are necessary to respond to the imminent threat; and
>
> (b) only if the activities carried out in co-operating and providing advice and assistance could not, in any circumstance, be authorised by an intelligence

---

511 Department of the Prime Minister and Cabinet *Addendum to Regulatory Impact Statement: Intelligence and Security Legislation – Information sharing arrangements and, assisting other organisations* (2016) at [27].

512 Department of the Prime Minister and Cabinet *National Security System Handbook* (2016) at [6].

513 Intelligence and Security Act 2017, s 10(1)(b)(iii) and s 10(2)(a–b).

514 Section 58(2)(a–g).

warrant issued for the purpose of performing a function under section 10 or 11; and

(c) subject to the restriction that any information obtained by the agencies in the performance of this function may not be used for any other purpose, except to the extent that the use for that other purpose is authorised by an intelligence warrant issued in the circumstances referred to in section 102(2)(a); and

(d) even though the co-operation, advice, and assistance might involve the exercise of powers or the sharing of capabilities that the agency is not, or could not be, authorised to exercise or share in the performance of its other functions.[515]

10.31. The departmental report on the Bill indicates these restrictions are designed to limit the exercise of this function to only situations where the Agencies could not otherwise obtain a warrant under urgency, for example, to support the cross-government response to an imminent terrorist threat that falls under the Agencies' national security objective.[516]

10.32. Section 14 empowers the Agencies to use their capabilities to support responses to imminent threats to the life or safety of New Zealanders or others when the Agencies would otherwise be unable to do so by limits placed on them under the ISA's warranting framework. While this does not address the "imminence" question raised by agencies, it does provide a basis for what activities fall within the "threat" component of this provision.

10.33. To be effective and enabling, we agree with a previous assessment by officials that s 14 needs to be broad to cover the potential range of circumstances and locations in which assistance might be required.[517] However, what may be lacking is a shared and clearly articulated understanding between agencies of what, when, and how intelligence collected by the Agencies to fulfil this function may occur and be conveyed across a range of potential threat scenarios.

10.34. On the issue of cooperation, the Cullen/Reddy report recommended that, when assisting other government agencies responding to imminent threats, "the Agencies should, as a matter of practice, develop joint operating protocols with other government agencies (for example, between the NZSIS and Police)".[518] In line with this recommendation, we feel the GCSB and NZSIS and wider agencies should reflect on how any such new or existing protocols capture the concept of "imminence" and the range of potential threat activities that may fall under this provision and how such protocols can be improved to support efficient and effective cooperation should such situations arise.

RECOMMENDATION	20

The Government Communications Security Bureau and the New Zealand Security Intelligence Service (the Agencies) and other domestic agencies with which the Agencies cooperate in

[515] For completeness, to support transparency and oversight, s 14(3) requires an Agency that undertakes any activity under s 14 to provide details of that activity to the responsible Minister and the Inspector-General as soon as is practicable and to report on the number of occasions it provided such assistance that year in its annual report. To date, both the GCSB and NZSIS have indicated in their annual reports that they have not provided assistance under s 14.

[516] Department of the Prime Minister and Cabinet *Departmental Report to the Foreign Affairs, Defence and Trade Committee* (2016) at [278].

[517] Above n, at [276].

[518] Cullen/Reddy report, recommendation 32.

order to respond to an imminent threat to life or safety under section 14 of the Intelligence and Security Act 2017 (ISA), should consider how any new or existing joint operating protocols capture the concept of an "imminent" threat to life or safety and the range of potential threat activity that may fall under section 14 and how they can be improved to support efficient and effective cooperation should such situations arise.

Assistance to give effect to an authorisation

10.35. There is a further provision in the ISA on cooperation between the Agencies and other organisations. Section 51 states:

> **Request for assistance to give effect to authorisations**
>
> (1) The Director-General of an intelligence and security agency may request assistance with giving effect to an authorisation from—
>
> (a) the New Zealand Police; or
>
> (b) any other organisation; or
>
> (c) any person.

10.36. Section 51 goes on to state that the request must specify the assistance required and be in writing and the person who assists is subject to the control of the Director-General of the Agency concerned may exercise the same powers as the Agency and has the same immunities as a person employed by the Agency.[519]

10.37. A provision enabling other people to assist in the execution of powers is a common feature of search and surveillance powers and is found in ss 113 and 114 of the Search and Surveillance Act 2012. It provides an ability for the relevant agency to seek assistance from others when executing a warrant. This enables, for example, an agency to seek assistance from a telecommunications company to help intercept communications under a warrant. As noted in chapter 3, it also provides a legislative vehicle for the NZDF and the New Zealand Customs Service (Customs) to provide assistance to the Agencies. No specific issues with s 51 have been raised during our review, although the legislative deficiencies surrounding the advice and assistance functions, as noted in chapter 3, are a broader issue that we consider should be addressed.

Information sharing under the ISA

10.38. Information sharing with domestic and foreign agencies is part of the statutory functions of the Agencies and subject to controls.

10.39. The Agencies are lawfully able to provide intelligence and analysis to people or classes of people authorised by the Minister, whether in New Zealand or overseas.[520] In the case of information sharing with overseas persons or authorities, the Minister must be satisfied that the Agencies will be acting in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.

---

[519] Intelligence and Security Act 2017, s 51(2)–(4).

[520] Section 10.

10.40. Information sharing also arises in respect of the Agencies' two other functions: to provide protective security services, advice and assistance and, more specifically in the case of the GCSB, to provide information assurance and cyber security services and advice.[521] This latter function includes identifying and responding to threats or potential threats to communications and information infrastructures of importance to New Zealand.[522] Cooperation with other entities is key to the exercise of both these functions. The sharing of cyber-security threat reporting may be authorised by the responsible Minister and, as with other information sharing, the Minister must be satisfied the GCSB is acting in accordance with New Zealand's human rights obligations where this reporting is shared with overseas persons or entities.[523]

10.41. As no particular issues were identified during our review in relation to information sharing to fulfil the protective security and information assurance functions of the Agencies, these functions are folded into consideration of intelligence sharing more generally.

Information sharing with domestic agencies

10.42. Information sharing operates in two directions – both to and from the Agencies. Much of the focus of information sharing, including in the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019 (the Royal Commission), is on the Agencies sharing information with others. However, the Agencies also receive information. Some of the information that is received is governed by Part 5 of the ISA, which is discussed in chapter 9. In other instances, the receipt of information is governed by the legislative frameworks of the providing agency. As noted in chapter 3, this may place constraints on the extent to which the Agencies receive information relevant to their functions.

10.43. A further preliminary point to note is that the legal framework within which the Agencies operate differs from that of other domestic agencies. The latter operate within the entire framework of the Privacy Act 2020 and all the privacy principles. The Agencies are not exempt from the Privacy Act; but some of the privacy principles do not apply to the Agencies, to enable them to perform their functions (namely information privacy principles 2, 3 and 4b).[524] Nevertheless, because of the secretive nature of the Agencies' activities, it is difficult for members of the public to know whether and when their privacy interests are implicated. Individuals can make requests under the Privacy Act to the NZSIS and the GCSB in relation to any of their personal information the Agencies hold, but they may not know or even suspect that the Agencies hold their information.[525] Individual complaints relating to privacy may be, and have been, made to both the Inspector-General and the Privacy Commissioner, but the secrecy on national security grounds over the information held by the Agencies means that the Privacy Commissioner is not as engaged with the Agencies as they are with other domestic agencies. As a result, the Agencies tend to work in a different informational sphere from other domestic agencies.

---

[521] Sections 11–12.

[522] Section 12(1)(b).

[523] Sections 12(5)(b) and 12(7).

[524] Privacy Act 2020, s 28. Information privacy principle 2 relates to the collection of personal information from the individual concerned. Information privacy principle 3 relates to taking reasonable steps to ensure the individual is aware that personal information is collected. Information privacy principle 4(b) requires the collection of personal information to be fair and not intrude to an unreasonable extent on the personal affairs of the individual concerned.

[525] See Inspector-General of Intelligence and Security *Complaints arising from reports of Government Communications Security Bureau intelligence activity in relation to the South Pacific, 2009-2015* (Public report, 4 July 2018).

10.44. The Royal Commission report discussed information sharing among domestic agencies, and its findings are in line with our conclusions.[526] We address such information sharing under four headings:

- the information sharing environment
- institutional, technical and legal barriers to the sharing of intelligence
- the 'need to share' not the 'need to know'
- the over-classification of intelligence.

Information sharing environment

10.45. The threat environment in New Zealand can no longer be considered benign. The information environment has been transformed through technological advances and a rise in cyber-borne threats. The face of terrorism is also changing with the prevalence of radicalised lone actors and small cells, compared to the large terrorist organisations of the past. Additionally, there is increased strategic competition in our region, and foreign interference and espionage activities are more subtle and less overt than they once were. The Agencies need to successfully assess the threats, intentions and capabilities of malicious actors because the consequences of failure could be significant.

10.46. This environment requires the Agencies to collaborate and share information with other agencies to anticipate and investigate the sources and nature of potential threats and opportunities. The information sharing framework needs to be enabling to facilitate the protection of New Zealand's interests and the identification and mitigation of threats. The changes required to meet the challenges of the new operating environment are not always legislative but can also be changes to organisational culture and practices.

Institutional, technical and legal barriers to the sharing of intelligence

10.47. It needs to be acknowledged that the Agencies' sharing of intelligence and analysis has improved over time. The ISA is generally enabling and not a hindrance to information sharing. Nevertheless, in our review, we found a number of barriers to sharing information domestically. Most of these are institutional or cultural barriers or technological and infrastructure barriers rather than legislative barriers.

10.48. Organisational cultures are a barrier to information sharing. In the Agencies, this results from the covert nature of the Agencies' work and a primary concern about breaching security procedures. In other domestic agencies, security issues may not be the prevalent focus. Where the Agencies are co-located with other domestic agencies, or where good personal relationships exist, such barriers can be reduced. We heard from those we interviewed that institutional barriers to sharing information could be overcome by domestic agencies working with their counterparts to ensure that the Agencies were able to release useful, timely and accurate intelligence and analysis at a classification level that could reach all the key decision makers.

[526] Royal Commission of Inquiry *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) at part 8, chapter 9 (*Royal Commission report*).

10.49. Even so, we also heard that the release of information by the Agencies to support assessments or decisions by other domestic agencies can sometimes take time because of the need to obtain the necessary sign-offs. This may be caused by classification levels, which we address below.

10.50. Some technological and infrastructural barriers to information sharing with domestic agencies were also identified. In some cases, the information technology (IT) systems of the various agencies are not able to exchange information at certain classifications, which can hamper information sharing. Moreover, human intervention is required to ensure that relevant information is put into the hands of those who need it. Staff in many agencies, including those on the Security and Intelligence Board, do not always have adequate access to sensitive compartmented information facilities (SCIFs) and therefore cannot always easily access, hold or discuss highly classified material. The technological barriers are compounded by the different computer infrastructure systems used for highly classified and other information.[527] No doubt, such differentiated systems are necessary, but the point is that information sharing may require a deliberate decision to share a particular piece of information that is of crucial importance in mitigating a threat. Information sharing may also require more resources being put into SCIFs, which are expensive to build and maintain, and security clearances for staff in other domestic agencies.

10.51. By and large, there are few legislative barriers to domestic agencies sharing information with the Agencies and, as discussed in chapter 9, direct access agreements facilitate this.[528] However, two notable exceptions were raised during our review.

10.52. First, the Customs and Excise Act 2018 enables Customs to collect and share information, but only for purposes under that Act and not, for example, for counterterrorism purposes or to fulfil the functions of the Agencies.[529] This means that New Zealand Customs is not able to copy and share information for a purpose related to the Agencies' functions, which results in less information getting to the Agencies than may be desirable. Non-specific information can be provided in Customs' intelligence reports, but this may leave out critical and valuable information that could assist the Agencies in countering threats.[530]

10.53. Second, as noted in chapter 9, Inland Revenue submitted that on occasion they come across information relevant to New Zealand's national security interests but are prevented from sharing such information with the Agencies because the permitted disclosures provisions of ss 18D to 18J of the Tax Administration Act 1994 make no provision for this. Information may be shared under the Targeting Serious Crime Approved Information Sharing Agreement, pursuant to s 18E(2) of the Tax Administration Act, and under s 140 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, but these contain criteria that if not met would prevent the disclosure of information. As recommended in chapter 9, consideration of a new permitted disclosure for national security interests, which is tightly controlled and with

527 Inspector-General of Intelligence and Security *A review of the New Zealand Security Classification System* (August 2018) at [181].

528 As noted in chapter 9, there is a direct access agreement between the NZSIS and Customs that covers CusMod, but this does not encompass all the information that Customs may hold.

529 Customs and Excise Act 2018, s 301(1) and (2).

530 We also note that, under information privacy principle 11(g) of the Privacy Act 2020, Customs may disclose personal information that is necessary to enable an intelligence and security agency to perform any of its functions, but this is subject to any statutory prohibition or restriction on sharing personal information and does not cover the NZDF. Given the extent of NZDF's intelligence capabilities, noted in chapter 3, this prevents Customs sharing personal information that may be relevant to NZDF's role.

monitoring mechanisms in place, would enable Inland Revenue to proactively provide relevant national security information on a case-by-case basis.

10.54. The sharing of information for national security purposes would be enhanced if both these legislative barriers were addressed.[531]

RECOMMENDATION 21

Amend the Customs and Excise Act 2018 to enable the New Zealand Customs Service to collect and share information pertaining to the functions of the Government Communications Security Bureau or the New Zealand Security Intelligence Service to facilitate cooperation under the Intelligence and Security Act 2017.

The need to share not the need to know

10.55. The traditional approach of intelligence agencies is to make sensitive information available to people who not only have the appropriate security clearances but also 'need to know' the information for the performance of their responsibilities. The deficiencies of such an approach were highlighted in the United States' Congressional investigations following the 9/11 terrorist attacks.[532] The alternative approach – the 'need to share' – promotes the collaborative sharing of timely and actionable intelligence among agencies to mitigate threats to life, property and national security.

10.56. The tension between the need to share and the need to know is not new.[533] On the one hand, intelligence is only valuable if it leads to something, whether better decision-making based on timely and accurate information, the protection of democratic institutions, improving public safety or identifying and addressing criminal behaviour. On the other hand, to the extent that information is more widely shared, there is an enhanced risk of that information falling into the wrong hands. We acknowledge that some information may need to have limited distribution in order to not compromise national security or operational effectiveness. However, it is important to reach the right balance between sharing and withholding information to help identify and mitigate or prevent events such as 9/11.

10.57. For many domestic agencies, relationships drive information sharing. Building trust may continue to help break down barriers to sharing, but it is likely to be insufficient. There are arrangements in place between parts of the Agencies and various domestic agencies to regularly share information. However, it was put to us that the Agencies need to move across the spectrum towards the 'need to share' and away from the 'need to know' given the increasingly interconnected nature of threats. We were told that the Agencies need to ask, 'how can I share?',

---

531 See recommendation 18 in chapter 9.

532 National Commission on Terrorist Attacks Upon the United States *The 9/11 Commission Report* (Washington: Government Printing Office, 2004) at 416–417.

533 Richard Best Jr *Intelligence Information: Need-to-Know vs. Need-to-Share* (Congressional Research Service, online, 6 June 2011).

rather than, 'why do I have to share?' As described by one of our consultees "… something has to emerge from the 'secret bubble' to be used". [534]

10.58. The Agencies have a legitimate concern about compromising sources and methods. However, an over-abundance of concern may constrain information sharing for the purposes of identifying and mitigating threats. The new classification system policy emphasises the importance of encouraging and supporting partnership and collaboration.[535] This suggests a greater focus on the need to share and consideration of how that can be factored into the sharing of information.

The classification of intelligence

10.59. A significant issue affecting the sharing of intelligence and analysis with domestic agencies is that it is classified at a level that means most employees in domestic agencies cannot view the material because they do not have the appropriate security clearances. Moreover, information may be compartmented for national security reasons and passed over with caveats or endorsements such as 'New Zealand eyes only' (NZEO), which restricts access even more.[536] A non-New Zealand citizen who is a resident may obtain a national security clearance where they have a checkable background. Waivers may be granted to non-New Zealand citizens to access and view NZEO material. However, we heard from some domestic agencies that the absence of security clearances for non-New Zealand citizens and the number of such people on their staff can pose issues.

10.60. A second issue is that, when intelligence is shared by foreign partners, the classification of the material remains that applied by the originating country. The recipient country handles the material at the equivalent classification within its own system – partners would not share information with New Zealand unless it provided the equivalent level of security.[537] In practice, and in order to avoid prejudice to the entrusting of information to the New Zealand government on a basis of confidence, the consent of the originating agency may, depending on the circumstances, need to be sought before partner information is shared beyond New Zealand government agencies.[538] The foreign partner control of historical information has been criticised by the Operation Burnham Inquiry[539] and by the Inspector-General during inquiries into Agency activities.[540] While the foreign partner control of information ensures New Zealand can protect and has control over the on-sharing of its own information, it also has the potential to operate as a constraint to sharing information that needs to be shared beyond the New Zealand government.

---

534 We acknowledge, however, that the Inspector-General of Intelligence and Security, Independent Police Conduct Authority and Office of the Inspectorate in their joint report did not find any reluctance from NZSIS to share their intelligence with appropriate agencies. See *Coordinated Review of the Management of the Lynn Mall Attacker* (14 December 2022) at [584].

535 NZSIS "New Zealand Government Information Security Classification System Policy 2022" Protective Security Requirements – Classification system (protectivesecurity.govt.nz).

536 GCSB *New Zealand Information Security Manual* Glossary of terms at [24.2].

537 Inspector-General of Intelligence and Security *A review of the New Zealand Security Classification System* (August 2018) at [191].

538 Consent may also be required if shared as part of legal proceedings.

539 Sir Terence Arnold, KNZM KC and Sir Geoffrey Palmer, KCMG AC KC PC *Report of the Government Inquiry into Operation Burnham* (17 July 2020) at [88]–[90].

540 Acting Inspector-General of Intelligence and Security *Report of Inquiry into the role of the GCSB and the NZSIS in relation to certain specific events in Afghanistan* (June 2020) at [203].

10.61. Third, the over-classification of information has also been identified as a risk by the Inspector-General of Intelligence and Security in their 2018 review of the New Zealand security classification system[541] by the Operation Burnham Inquiry[542], and the Royal Commission.[543] The Inspector-General noted that classification systems have an "inherent bias towards over-classification" and that security bureaucracies give officials little reason to avoid or challenge over-classification and noted the harmful effects of this for transparency.[544] More specifically, over-classification of information can make it difficult to provide accurate and timely information to decision-makers or to staff in domestic agencies to help inform them of the current threat environment. The more information that can be released at a lower classification, the easier it will be for the information to be disseminated to not only inform agencies of the threat environment but also provide them with intelligence that they can act upon, either as leads that can be followed up or for law enforcement purposes.

10.62. The Agencies are seeking to address past criticisms and have responded to recommendation 9 of the Royal Commission through an updated New Zealand Government Information Security Classification System Policy 2022, which cautions against over-classification. This is accompanied by a suite of learning tools and guidance to help those classifying information to do so appropriately. However, it is recognised that, even with a clear classification system, an overly cautious approach may still lead to over-classification. Moreover, although we have focused here on over-classification, under-classification of information can also pose real risks to New Zealand's national security interests. The Information Security Classification System Policy therefore emphasises "appropriate" classification and provides guidance on how to assess the potential harm and impact if the information is compromised.

10.63. The Information Security Classification System Policy also seeks to establish a policy framework for declassifying information. The development of a consistent and comprehensive approach to declassification is welcome. In addition, the revision of documents to redact classified material, or 'sanitising' documents, so that information can be viewed at a lower level of classification without compromise of sources, methods or legitimate State interests, may also help broaden the permissible scope of information sharing with domestic agencies.

Conclusions on information sharing with domestic agencies

10.64. Information sharing between domestic agencies plays an essential role in facilitating the protection of New Zealand national security interests and the identification and mitigation of threats. The barriers to sharing of information are largely institutional or cultural rather than legislative. In particular, there should be a greater focus on the need to share, rather than the need to know, and this should apply across the government as a whole.

10.65. The classification system plays a role in helping to facilitate information sharing with domestic agencies. The use of appropriate classification markings (in particular, not over-classifying), redaction of classified material and declassification can help domestic agencies act on the information.

---

[541] Inspector-General of Intelligence and Security *A review of the New Zealand Security Classification System* (August 2018).

[542] Sir Terence Arnold, KNZM KC and Sir Geoffrey Palmer, KCMG AC KC PC *Report of the Government Inquiry into Operation Burnham* (17 July 2020) at [85].

[543] Royal Commission report, at part 8, chapter 9, [29]–[33] and [57].

[544] Inspector-General of Intelligence and Security *A review of the New Zealand Security Classification System* (August 2018) at [106]–[107].

RECOMMENDATION 22

The Government should drive an approach to information sharing among domestic agencies that appropriately balances the need to share with the need to know to facilitate the protection of New Zealand's national security. This should include implementing the Information Security Classification Policy 2022 in a way that ensures the appropriate classification of information and encourages the declassification of information so that it can be used to respond to national security concerns.

Information sharing with foreign agencies

10.66. As has been noted, information sharing with foreign partners is a crucial element to the Agencies' operational activities.

With whom does New Zealand share intelligence?

10.67. The Agencies may provide intelligence to any overseas public authority authorised by the responsible Minister. New Zealand belongs to the Five Eyes relationship, which provides a platform for sharing intelligence.[545] New Zealand is both a provider and a recipient of intelligence, analysis and assessment. As we noted in chapter 3, it is dwarfed by the intelligence collection capabilities of its partners. However, we understand that it nevertheless contributes significantly in some discrete areas and provides certain high-value intelligence to the Five Eyes. It may also contribute to what the United States of America refers to as 'burden sharing' or a division of labour among the most trusted and capable allied foreign intelligence services.[546]

10.68. Sharing intelligence with foreign partners may be undertaken to fulfil the functions of the Agencies. This includes sharing intelligence on threats to New Zealand's national security, to respond to international security threats and to identify and mitigate cyber-security threats. Each Agency tends to have relationships with agencies in foreign partner countries that stem from their different functions. For example, signals intelligence (SIGINT) reporting is routinely exchanged among the SIGINT agencies of the Five Eyes (GCSB in New Zealand's case) and methods and techniques of SIGINT collection and analysis are shared where relevant and where the originator of the information agrees. Contacts among the Five Eyes partners in particular are extensive and regular and include not only information exchange but also joint training and other forms of cooperation.

10.69. Members of the Five Eyes are known to cooperate with other parties in Europe and Asia.[547] Among the international intelligence community, the sharing of raw data or unfinished intelligence takes place where there is a relationship of trust that the partner can provide the necessary security, such as occurs within the Five Eyes.[548] However, more frequent is the sharing

---

545 An intelligence partnership between Australia, Canada, New Zealand, the United Kingdom and the United States of America (the United States).

546 Michael DeVine *United States Foreign Intelligence Relationships: Background, Policy and Legal Authorities, Risks, Benefits* (Congressional Research Service, 15 May 2019) at 14.

547 Above n, at 14.

548 Above n, at 12.

of intelligence analysis or the 'finished' product of intelligence gathering.[549] Foreign partners may also request New Zealand's consent to on-share New Zealand sourced intelligence.

Framework for sharing with foreign partners

10.70. The Agencies may only provide intelligence and analysis to persons authorised by the responsible Minister.[550]

10.71. Each of the Five Eyes and other foreign intelligence agencies use and disseminate intelligence in accordance with their own national legislation and policies. The ISA requires that the Agencies, in sharing information and cooperating with foreign agencies, act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law. This means in essence that the human rights records of agencies with whom information is shared must be examined to ensure the information is not used later to facilitate human rights abuses and was not obtained through serious human rights violations.

10.72. A ministerial policy statement (MPS) on cooperation with overseas public authorities provides the general requirements for the on-sharing of New Zealand intelligence. The MPS was significantly amended in April 2021 and was reissued unchanged in March 2022. Amendments to a MPS are subject to consultations with the Inspector-General. We were told that, in this case, there was wide consultation, including with the Ministry of Foreign Affairs and Trade (MFAT), Ministry of Justice, Privacy Commissioner, Human Rights Commission, Police, Ministry of Defence, NZDF and Customs. On the recommendation of the Inspector-General in her report on the US Senate inquiry into the CIA rendition and detention programme, public consultation was also undertaken. The MPS on cooperation with overseas public authorities directs the Agencies to have internal policies, procedures and guidance for staff. The Agencies have a joint policy statement (JPS) on managing human rights risks in overseas cooperation. Although classified, a summary of the JPS has been released under the Official Information Act 1982.[551] The revised JPS was issued in December 2021.

10.73. The MPS sets out the requirements for undertaking a human rights risk assessment to ensure compliance with New Zealand's human rights obligations. This involves the completion of a human rights risk assessment before sharing intelligence or analysis or being able to use intelligence received. The Agencies must assess any risks associated with the proposed cooperation in light of the foreign party's general human rights practices. Assessments are always case specific and focus on human rights risks relevant to the Agencies' functions and the proposed cooperation.

Human rights risk assessment framework

10.74. The MPS's requirement for a risk assessment framework for the Agencies' foreign cooperation sets out four components: (i) general risk; (ii) risk arising from the proposed cooperation; (iii) opportunity for mitigating risk and (iv) response to a real risk of a human rights breach.[552]

---

549 Above n, at 12.

550 Intelligence and Security Act 2017, s 10(1)(b)(iii).

551 GCSB and NZSIS *Summary: Joint Policy Statement on Rights Risks in Overseas Cooperation* (proactive release date, 2 June 2022).

552 Minister Responsible for the GCSB and NZSIS *Ministerial Policy Statement on Cooperation with overseas public authorities* (online, 1 April 2021) at [21]–[24] (*MPS on Cooperation*).

10.75. The MPS specifies the human rights information that must accompany an application for ministerial authorisation. This includes:

- the purpose of the intelligence sharing and how it contributes to the Agency's objectives and functions
- any particular human rights risk associated with the proposed cooperation and the likelihood of such a risk occurring
- how any identified risks might be mitigated.

10.76. The MPS also specifies factors the relevant Agency must include in assessing the human rights practice of a country or public authority. This includes, among other things, a foreign party's human rights record, ratification of relevant international treaties and independence of the judiciary.[553] The MPS also requires the Agencies to have regard to any information available from MFAT on human rights.[554] The Agencies would be expected to consult credible sources such as United Nations documents, Amnesty International or Human Rights Watch in order to complete the risk assessment.[555]

10.77. The MPS directs the Agencies to consider whether the proposed cooperation might result in a real risk of significantly contributing to or being complicit in a breach of human rights. The likelihood of human rights breaches in connection with overseas public authorities are assessed, and the Agencies must take a precautionary approach to this assessment.[556] Mitigations may need to be adopted to lower risk (such as conditions on use of intelligence, caveats requiring the recipient to seek permission for certain uses of the Agencies' intelligence or to on-share it or redaction of identifying information).[557] If there is a real risk of significantly contributing to or being complicit in a breach of human rights, cooperation must be refused or referred to the responsible Minister for decision.[558] Human rights abuses in a foreign country are therefore not an absolute bar to cooperation.

Human rights risk assessments undertaken by the Agencies

10.78. We understand that the Agencies undertake the human rights risk assessments in a diligent and comprehensive manner. The Agencies engage with MFAT, where it assists when completing the assessments and use a wide variety of sources. The human rights risk assessment process enables human rights risks to be managed so the Agencies can contribute to international security by being able to share the intelligence they collect with foreign partners, including their Five Eyes partners.

10.79. In our review, we considered whether the centralisation of human rights risk assessments is best placed in the Agencies. On the one hand, centralisation of human rights risk assessments within an agency that has broad understanding of international human rights as well as the human

553 MPS on Cooperation, Appendix One.

554 MPS on Cooperation, at [12].

555 In her public report on the US Senate inquiry into CIA detention and rendition programme, the Inspector-General of Intelligence and Security set out the various sources that could provide information about a State's human rights record: Inspector-General of Intelligence and Security *Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001-2009* (31 July 2019) at [216].

556 MPS on Cooperation at [22].

557 GCSB and NZSIS *Summary: Joint Policy Statement on Rights Risks in Overseas Cooperation* (proactive release date, 2 June 2022) at [6].

558 MPS on Cooperation at [24].

rights situation in particular countries, such as MFAT, could bring rigour and impartiality to the assessments. It could help avoid institutional bias in the assessments in favour of information sharing. On the other hand, having the Agencies complete the assessments helps ensure the Agencies consider human rights throughout the information sharing process rather than just at the stage of obtaining a standing authorisation to share information with a foreign partner. This mainstreaming of human rights within the operational work of the Agencies has value. It enables the Agencies to consider on an ongoing basis the human rights situation in the country with which information is shared. This is particularly important if the underlying conditions in a standing ministerial authorisation change or the human rights situation in a country no longer justifies the continuation of the authorisation.

Ministerial authorisations and approved parties

10.80. The ISA requires Ministerial authorisation for sharing intelligence and analysis with a foreign party. This can be on a one-off basis or on the basis of a standing authorisation, where the country has a good human rights records and strong human rights institutions. Figures released under the Official Information Act 1982 give an idea of the scale of foreign intelligence sharing, with approximately 1,500 human rights risk assessments undertake (the majority by the GCSB) to support information sharing over a 3-year period.[559]

10.81. The JPS on cooperation indicates that the Agencies may request that the Minister grant "Approved Party status to an Authorised Party whose human rights situation is broadly comparable to New Zealand's".[560] According to the JPS, the Agencies can cooperate with approved parties without undertaking human rights risk assessments in most cases. However, approved party status may need to be reviewed or a human rights risk assessment conducted if there are increased risks for ongoing cooperation from changes to the foreign party's law, policy or practice or where there is evidence they are responsible for a significant human rights breach. It is not clear from public documents which countries are authorised parties and which are approved parties. Standing authorisations are reviewed regularly,[561] but as the Inspector-General has noted:[562]

> It is essential that the New Zealand intelligence and security agencies and other relevant Government agencies have in place structures, policies and practices (including regular monitoring) to detect any unlawful conduct by partner agencies and prevent New Zealand involvement, direct or indirect, in that conduct.

10.82. There are also transparency concerns. The period of a standing ministerial authorisation is not public, nor whether review is necessary and adequate if circumstances change. In general, there is a lack of transparency about the special status of approved parties and the criteria for determining approved party status. This is concerning given the potential open sharing of information with approved parties.

---

559 Information provided by GCSB and NZSIS, current as of 15 November 2021.

560 GCSB and NZSIS *Summary: Joint Policy Statement on Rights Risks in Overseas Cooperation* (proactive release date, 2 June 2022) at [4].

561 MPS on Cooperation at [6].

562 Inspector-General of Intelligence and Security, *Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001-2009*, 31 July 2019 at [330].

Intelligence sharing and torture and other serious human rights abuses

10.83. The prohibition against torture or cruel, inhuman or degrading treatment or punishment is a significant international legal obligation with which New Zealand must comply and from which no derogation is permitted. There are two ways in which the sharing of intelligence may implicate the prohibition against torture: the outgoing sharing of intelligence that leads to the commission of torture and other serious human rights abuses and the incoming receipt of intelligence that has been obtained by torture. Internationally, there have been notable serious allegations of intelligence cooperation contributing to torture and human rights abuses, leading to inquiries in Canada,[563] the United Kingdom[564] and the United States of America among others.[565] New Zealand has not been immune from such inquiries.[566]

10.84. The MPS on cooperation covers both outgoing and incoming intelligence sharing. Where the sharing of intelligence will significantly contribute to, or amount to complicity in, a breach of human rights, cooperation must be refused or referred to the responsible Minister for a decision.[567] The Agencies are alive to the possibility that intelligence they share may contribute to human rights abuses and seek to mitigate the risk in accordance with the MPS and their internal policies.

10.85. The MPS and JPS on cooperation also address the use of information where there is a real risk that it may have been obtained by torture. The MPS acknowledges the unreliability of information obtained through torture and imposes limitations on when such information can be used by the Agencies.[568] The relevant Director-General may approve the use only in exceptional circumstances, such as to prevent loss of life, significant personal injury or threat to critical national infrastructure.[569] The use of the information must not contribute to a further serious breach and must be notified to the Minister and the Inspector-General.

10.86. The Inspector-General's inquiries related to the US Senate inquiry into the CIA detention and rendition programme and Afghanistan, the Operation Burnham Inquiry and the government's response to them have heightened the Agencies' awareness of the risks that information sharing may contribute to human rights abuses. Consequently, there is a requirement in the MPS that information that may have been obtained as a result of torture (or any other serious human rights breaches) may only be used in the rarest and most exceptional circumstances. The MPS is supplemented by the JPS on cooperation. The Inspector-General's last two annual reports have

---

563 *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (Privy Council, Ottawa, 2006), which led ultimately to the Avoiding Complicity in Mistreatment by Foreign Entities Act SC 2019 c 13.

564 The Joint Committee on Human Rights *Allegations of UK Complicity in Torture – Twenty–third Report of Session 2008–09* (House of Lords, 21 July 2009).

565 Dianne Feinstein and the Select Committee on Intelligence *Report of the Senate Select Committee on Intelligence Committee Study of the Central Intelligence Agency's Detention and Interrogation Program* (online, 9 December 2014).

566 Inspector-General of Intelligence and Security *Report into whether NZSIS and GCSB had any connection to the CIA's "enhanced interrogation", detention and rendition programme in Afghanistan between 2001–2009* (31 July 2019); Inspector-General of Intelligence and Security *Report of Inquiry into the role of the GCSB and the NZSIS in relation to certain specific events in Afghanistan* (June 2020); Sir Terence Arnold, KNZM KC and Sir Geoffrey Palmer, KCMG AC KC PC *Report of the Government Inquiry into Operation Burnham* (17 July 2020).

567 MPS on Cooperation at [24].

568 United Nations Office of the High Commissioner for Human Rights "Torture during interrogations – Illegal, immoral and ineffective" (11 October 2017) (https://www.ohchr.org/).

569 GCSB and NZSIS *Summary: Joint Policy Statement on Rights Risks in Overseas Cooperation* (proactive release date, 2 June 2022) at [9]; MPS on Cooperation at [27].

flagged outstanding policy issues with the JPS regarding the handling of reports likely to have been obtained by torture.[570] The question of whether, and the circumstances in which, the Agencies could share information that may have been obtained through torture was closely examined during the review of the MPS. Nevertheless, given the abhorrence that New Zealanders feel towards the practice of torture, this is an issue that should be kept under review.

Third-party rule

10.87. The third-party rule prohibits the disclosure of information shared between agencies to a third party without the prior consent of the state from which the information originated.[571] This means that if New Zealand shares intelligence with a Five Eyes partner, that partner cannot on-share the intelligence to a third party without New Zealand's consent. The third-party rule ensures that the Agencies maintain a degree of control over the information that is being provided to or by partners and can condition consent, such as asking that a particular form of words be used or that the source of the intelligence be protected.

10.88. The third-party rule was raised in the 2021 annual report of the Inspector-General, who had a different view from that of the Agencies as to whether explicit ministerial consent was required for the Agencies to agree to a partner on-sharing intelligence to a third party.[572] The Inspector-General considered that s 10 requires there to be a ministerial authorisation for any third-party recipient of New Zealand intelligence and that the absence of this was a matter for our review.

10.89. The statutory safeguard in s 10 of the ISA requires the Minister to be satisfied that, in providing intelligence and analysis to overseas people, the relevant Agency will be acting in accordance with New Zealand law and all human rights obligations recognised by New Zealand law. This safeguard ensures that the Minister is aware of any legal, human rights, political and reputational risks involved in Agencies sharing intelligence with specific countries before the intelligence is made available. Ministerial oversight serves to manage risks, including human rights risks, arising from the sharing of intelligence. The MPS issued by the Minister and the current JPS on cooperation approved by the Minister help manage risk through a risk assessment framework. Cooperation with a foreign party, which would include sharing information with a third party, is considered and approved on the basis of the level of risk, with ministerial authorisation required at the highest risk level where there is a real risk of contributing to human rights breaches.[573]

10.90. The Minister must be satisfied the human rights considerations have been taken into account and addressed before any permission will be granted to share intelligence with a foreign partner. Where the Minister does not expressly consent to the on-sharing by a foreign partner of New Zealand intelligence to a third party, the Minister essentially delegates this task to the Agencies (including by providing a standing ministerial authorisation), and there is a risk, albeit small, that the Agencies share intelligence in a way that calls into question New Zealand's human rights obligations.

---

570 Inspector-General of Intelligence and Security *Annual Report for the year 1 July 2021 to 30 June 2022* (November 2022) at 7 and Inspector-General of Intelligence and Security *Annual Report for the year 1 July 2020 to 30 June 2021* (November 2021) at 6–7.

571 Michael DeVine *United States Foreign Intelligence Relationships: Background, Policy and Legal Authorities, Risks, Benefits* (Congressional Research Service, 15 May 2019) at 15.

572 Inspector-General of Intelligence and Security *Annual Report For the year 1 July 2020 to 30 June 2021* (11 November 2021) at 7.

573 GCSB and NZSIS *Summary: Joint Policy Statement on Rights Risks in Overseas Cooperation* (proactive release date, 2 June 2022) at [5]–[7].

10.91. We acknowledge that the Agencies have robust policy settings to address this risk. However, a specific requirement in the ISA confirming that, in such circumstances, the Agencies must act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law may assist in providing greater clarity in this regard. In addition, we are not aware of any reporting to the Minister of the number and identity of recipients of New Zealand-sourced intelligence and analysis provided under the third-party rule. Such reporting would help ensure the Minister is satisfied the safeguards in s 10, the MPS and the JPS on cooperation are being implemented appropriately.

Conclusions on information sharing with foreign agencies

10.92. The MPS and associated JPS on cooperation have recently been revised and reissued. Some of the amendments were in response to the recommendations of the Operation Burnham Inquiry and the Inspector-General inquiries into Afghanistan and US Senate inquiry into CIA's detention and rendition programme. We recommend the next periodic review of the MPS re-evaluate the MPS in light of experiences with implementing it and its associated JPS.

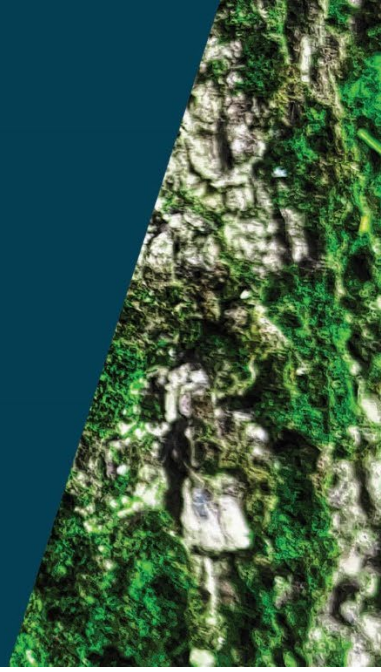
10.93. Before that, however, action can be taken to enhance transparency in how the MPS is operationalised. Information should be provided publicly on the criteria on which approved party status is granted, the time period for which a standing ministerial authorisation is approved, whether the time period is adequate if circumstances change and factors that would trigger a review of the status. Such information could be made public. Without such transparency, information sharing with foreign partners is essentially outside the public gaze. This breeds distrust over an activity that may enhance international security.

RECOMMENDATION 23

With respect to the recently revised and reissued ministerial policy statement (MPS) on cooperation with overseas public authorities, which sets out the general requirements for the on-sharing of New Zealand intelligence:

a. To improve transparency relating to information sharing with overseas public authorities, the public should be provided with information about:
   i. the criteria used to grant 'approved party' status for sharing intelligence with foreign partners
   ii. the time period for which a standing ministerial authorisation for sharing intelligence is approved
   iii. whether the time period is adequate if circumstances change
   iv. what factors would trigger a review of the status of the overseas public authority with which intelligence is shared.

b. The MPS on cooperation should be re-evaluated during its next periodic review in light of further experience with implementing the MPS and the related joint policy statement on managing human rights risks in overseas cooperation.



CHAPTER 11
Assessing and using intelligence

Introduction

11.1. Chapter 10 considered the sharing of information with agencies, both domestic and foreign. One point noted was that the sharing of information makes no sense unless it can be used by the agencies with whom it is shared. In this chapter, we deal with the use of intelligence collected by the two intelligence and security agencies (the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS), referred to as 'the Agencies') including for assessment purposes.

11.2. We address the following issues.

- The assessment of intelligence and whether the products that domestic agencies produce are effective in helping the government to protect the country against threats to national security.
- If intelligence identifies threats to Aotearoa New Zealand's national security, including the security of critical infrastructure, to what extent can the agencies take action to mitigate, reduce or disrupt these threats and prevent them from causing harm to New Zealand or New Zealanders.
- The process of vetting candidates for security clearances, which is part of the protective security functions of the NZSIS, can obtain information of a highly sensitive and personal nature to the individual candidate, and their family, friends and referees. The question has arisen as to how such information can be used, including for law enforcement purposes or to prevent threats to life.

Assessment of intelligence

11.3. Chapter 10 looked at the sharing of information by the Agencies with other partners including domestic agencies. It raised the point that the requirement for security clearances, and the level of classification of material, may in some circumstances limit the sharing of information and, in turn, the use of that information by decision-makers. This section looks at the use of information received from the Agencies for assessment of threats to New Zealand's national security and assessments that aim to help decision-makers in understanding the context in which their decisions are made. This focus is in line with the views of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019 (the Royal Commission), which considered in its report that "greater coordination and integration of the assessment function is required".[574]

[574] Royal Commission of Inquiry *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) at part 8, chapter 4 [34] (*Royal Commission report*).

11.4. This section considers the National Assessments Bureau (NAB) and the Combined Threat Assessment Group (CTAG), the recommendations of the Cullen/Reddy Review and the Royal Commission, their implementation and the issues that have been raised during the review.

National Assessments Bureau

11.5. The role and functions of the NAB have already been explained in chapter 3. As described, the NAB is New Zealand's primary assessments agency providing independent and impartial assessment of intelligence to the Prime Minister and Ministers, as well as government departments. It sits within the Department of the Prime Minister and Cabinet (DPMC). As the Cullen/Reddy report noted:[575]

> oversight occurs at many levels: from internal controls and compliance mechanisms to ministerial authorisation of the Agencies' activities and appropriate involvement of independent institutions … Not all checks and balances are readily apparent; some are built into the organisational structure of the system. For example, intelligence collection, assessment and policy formation have historically been separated. This helps to ensure objective assessments that are not tailored to support the pre-conceptions of collection agencies or the policy preoccupations of the day.

11.6. Given the role of intelligence assessment as a check in the system, the Cullen/Reddy review recommended that New Zealand's central intelligence assessment function be given a statutory basis. As a result, the Intelligence and Security Act 2017 (ISA) provides for the intelligence assessment function that is performed by the NAB.[576] We provide observations on the relevant sections in the ISA (s 233 and s 234) and consider the recommendations of the Cullen/Reddy review and the Royal Commission.

11.7. First, the structure contemplated by the ISA is unusual. As explained in chapter 3, the NAB is not named in the ISA. Under s 233, the chief executive of DPMC is responsible for the performance of three functions: providing intelligence assessments to Ministers and others, advising Ministers on priority setting for intelligence collection and analysis, and advising on best practice in relation to intelligence assessment. However, the chief executive is prohibited from performing the first and third of these functions personally but rather designates an employee to perform them. That employee is directed under s 234 to act independently in the performance of those two functions. The designated employee heads the NAB, which sits within the National Security Group in DPMC and reports to the deputy chief executive, National Security Group.

11.8. This structure has obvious inherent tensions, for example, in relation to the allocation of resources within DPMC. But the larger issue is whether it is appropriate to locate a body that is charged with performing an independent intelligence assessment function within the department that supports the Prime Minister, given the Prime Minister's overall responsibility for national security and intelligence. The danger is that policy considerations may influence, or at least be perceived to influence, intelligence assessments, thus undermining the independence of the function. Arguably, the NAB's independence would be reinforced from a public perspective if it was a stand-alone agency or located elsewhere, with protections for its independence from

---

575 Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM *Intelligence and Security in a Free Society – Report of the First Independent Review of Intelligence and Security in New Zealand* (February 2016) at [4.6] (*Cullen/Reddy report*).

576 Intelligence and Security Act 2017, ss 233–234.

policy and collection counterparts. Presumably, the placement of the NAB will be considered in the context of DPMC's work on the overarching machinery of government issues.

11.9. This leads to the second point, which is that in contrast to the detail in the ISA in relation to the Agencies, the Commissioners of Intelligence Warrants, the Inspector-General of Intelligence and Security (Inspector-General) and the Intelligence and Security Committee, the ISA contains little detail on the independent intelligence assessment function. The Cullen/Reddy review recommended the NAB be brought within the mandate of the Intelligence and Security Committee, which may have filled some gaps, but that did not occur. The Cullen/Reddy review also suggested that, to promote greater public engagement with national security issues, some of the NAB's assessments could be released publicly but, as far as we are aware, that has not happened. The NAB has released a limited amount of information under the Official Information Act 1982.

11.10. The Directors-General of the Agencies are required "to regularly consult with the Leader of the Opposition to keep him or her informed about matters relating to the agency's functions".[577] One of the issues raised with us is whether a similar provision should be in the ISA in relation to the NAB. A statutory requirement to brief the Leader of the Opposition from time to time would reflect that the NAB is required to act independently and the importance of ensuring continuity in the understanding of the international and national security threatscape in the event of a change of government. The Director of the NAB currently seeks permission from the Prime Minister to brief the Leader of Opposition on a case-by-case basis. We recommend that this be regularised, and the Director of the NAB be placed under the same obligation as the Directors-General of the Agencies.

RECOMMENDATION **24**

Amend the Intelligence and Security Act 2017 (ISA) to require the Director of the National Assessments Bureau to regularly consult the Leader of the Opposition, in line with the obligations placed on the Directors-General of the Government Communications Security Bureau and New Zealand Security Intelligence Service under section 20 of the ISA.

Combined Threat Assessment Group

11.11. As outlined in chapter 3, CTAG is an interagency group hosted by the NZSIS. It provides assessments to inform the national security system and wider government agencies of the physical threat posed to New Zealanders and New Zealand interests from terrorism, violent extremism in advance of terrorist acts, and violent protest and violent crime abroad. CTAG produces an annual national terrorism threat assessment, which is a statement about the likelihood of a terror attack occurring in New Zealand. This and other periodic assessments consider the intent and capability of persons to conduct terrorist attacks and relevant international threat factors.

[577] Intelligence and Security Act 2017, s 20.

Issues relating to assessment

Placement of the Combined Threat Assessment Group

11.12. The Cullen/Reddy review recommended a review of the placement of CTAG within the NZSIS and whether it might more appropriately be situated within the NAB.[578] This review took place in 2018 and recommended retaining the structural placement within the NZSIS due to the benefits both to CTAG's mission and for the national security system.[579] The recommendation was accepted by the government. We were told that, in practice, although both the NAB and CTAG focus on domestic and global aspects of terrorism and violent extremism, they differ in relation to the scope and purpose of their products. The NAB concentrates on the strategic level assessments and CTAG focuses on tactical and operational level assessments to inform decision-making including through horizon-scanning insight reports. In essence, they produce reporting to cater to different customer requirements.

11.13. The Royal Commission reached a similar conclusion as the Cullen/Reddy review. It concluded:[580]

> Greater coordination and integration of the assessment function is required. One way of achieving this would be to co-locate or combine the National Assessments Bureau and the Combined Threat Assessment Group.

Presumably, this issue will be reconsidered in the context of DPMC-led machinery of government work.

11.14. The Royal Commission considered that the government's intelligence assessment functions were not well situated to providing assessments of emerging threats. The Royal Commission attributed this to the NAB's customer focus and limited resources and, in part, to CTAG's short-term and tactical focus.[581] It also expressed concern over the lack of a regular strategic assessment of the New Zealand threatscape,[582] and the lack of a medium to long-term horizon scanning capability to identify emerging threats in order to strategically determine priorities and position resources.[583] The Royal Commission recommendations in response to this finding focused in part on the organisational structure of the intelligence community. Again, we assume these issues will be addressed in the work being undertaken by DPMC.

An annual threatscape report

11.15. The Royal Commission saw its principal recommendations as leading to, among other things, "well-informed ministers (with thorough understanding of the immediate, medium-term and longer-term terrorism risks and threats)". In particular, the Royal Commission recommended the government require in legislation that:[584]

---

578 Cullen/Reddy report, at [4.34].
579 Simon Murdoch *CTAG 2018: Its placement in New Zealand's counter-terrorism system architecture and its location; an independent view* (July 2018).
580 Royal Commission report, at part 8, chapter 4.8 [34].
581 Royal Commission report, at part 8, chapter 15 [57].
582 Royal Commission report, at part 8, chapter 4.8 [35]–[39].
583 Royal Commission report, at part 8, chapter 4.8 [40]–[44].
584 Royal Commission report, at part 10, chapter 2 recommendation 17.

a. the Minister for National Security and Intelligence publish during every parliamentary cycle the National Security and Intelligence Priorities and refer them to the Parliamentary Intelligence and Security Committee for consideration;

b. the responsible minister (Recommendation 1) publish an annual threatscape report; and

c. the Parliamentary Intelligence and Security Committee receive and consider submissions on the National Security and Intelligence Priorities and the annual threatscape report.

We now turn to this question.

11.16. The NAB is currently the only agency to prepare reports giving a broad assessment of threats to national security. NAB's function of providing intelligence assessments on national and international security was given a statutory basis in 2017 under s 233(1)(a) of the ISA.

11.17. By way of background, in 2012 and in response to recommendations of independent reviews, the NAB coordinated and produced for the first time a series of independent strategic intelligence assessments to accompany advice from DPMC to Ministers on setting intelligence priorities. Then, in 2015, 2016 and 2018, at the request of the Security Intelligence Board, it prepared a strategic assessment report that scanned the horizon for major changes to New Zealand's national and international security. These assessments also accompanied advice from DPMC on setting the National Security and Intelligence Priorities but were not publicly released.

11.18. Unlike the NAB, the CTAG and NZSIS functions related to assessment and reporting are not set out in the ISA. CTAG, by virtue of its focus on terrorism, provides reporting focused on this priority. The 2021 Threat Assessment[585] was accompanied by the Threat Insight on New Zealand's Violent Extremism Environment.[586] This latter document is more forward looking and considers trends and the threat outlook of violent extremism. Both CTAG documents were proactively released under the Official Information Act 1982, with some redactions. We understand the NZSIS is preparing its first public threat environment report, which will analyse national security threats within the focus of NZSIS, such as counterterrorism.

11.19. We also considered whether any other agency produced a threatscape report. As we note in chapter 3, the Ministry of Defence is under a statutory obligation to provide a defence assessment under s 24(2) of the Defence Act 1990. This is generally made public and produced every five years. It is described as "a comprehensive review of the challenges to New Zealand's strategic defence interests", focusing largely on external threats.[587]

11.20. We note that, in November 2022, the nine government agencies that make up the Security and Intelligence Board released a draft national security long-term insights briefing for public comment. This looks at "key global trends that will influence New Zealand's national security over the next 10 to 15 years, national security risk and challenges over this period, and key

---

[585] Combined Threat Assessment Group *Threat Assessment: New Zealand Terrorism Threat Level Remains at MEDIUM* (online, 6 December 2021).

[586] Combined Threat Assessment Group *Threat Insight: New Zealand's Violent Extremism Environment* (21 November 2021). The Combined Threat Assessment Group (CTAG) also produces other insights, for example, a report into New Zealand's terrorism threat environment. This is referred to in the Combined Threat Assessment Group *Threat Insight: New Zealand's Violent Extremism Environment* (21 November 2021) at [33].

[587] For the most recent assessment see, Ministry of Defence *Defence Assessment 2021: He moana pukepuke e ekengia e te waka / a rough sea can still be navigated* (December 2021).

features that could support national security into the future".[588] The long-term insights briefings are required by the Public Service Act 2020 and are to be independent of government and not government policy.[589] The choice of national security as a topic for the national security long-term insights briefing was inspired by the intent of the recommendations of the Royal Commission in seeking to share more information with members of the public and engage with them on their concerns.

11.21. The Royal Commission provides extensive commentary on the gaps in assessment reporting and found that "greater coordination and integration of the assessment function is required".[590] Having considered the various outputs of agencies, we believe that the government does not currently produce a single report that conforms to what the Royal Commission would term an 'annual threatscape report'. Such a report has not been consistently provided to Ministers to help them set intelligence priorities.

11.22. The public release of the CTAG documents shows the advantages of increased transparency on New Zealand's threat environment. They provide greater insights into threats, analysis of trends and a future outlook, which can improve the public's understanding of one threat to national security. Together with the NAB's strategic assessment reports between 2015–2018 (which, as noted, were not made public), these independent assessment reports come closer to what is available to the public in other countries on threats to their national security.[591] However, public release should not rely on a decision to proactively release a particular document, which in any case may not include all relevant information on different threats to New Zealand's national security.

11.23. The review accepts that work is under way to increase public understanding of the threats to New Zealand's national security. However, we agree with the Royal Commission that a legislative requirement to produce and publish an annual independent assessment report. This should cover the threats to New Zealand's national security, the threat environment, trends and outlook. It would ensure the robustness of the intelligence priority-setting process and enhance parliamentary and public understanding of threats to New Zealand's national security. This in turn would enhance social licence for the Agencies and the wider national security system. Increasing engagement with the public on national security threats was a conclusion of the Cullen/Reddy review,[592] raised by the Royal Commission, and still has not been fully implemented.

RECOMMENDATION 25

The National Assessments Bureau should produce a classified independent annual threatscape report to inform the intelligence priority-setting process by Ministers. The Bureau should also publish an unclassified version of the annual threatscape report, including to support a public hearing and submissions to the Intelligence and Security Committee on New Zealand's changing threatscape.

---

588 New Zealand Government *Let's talk about our national security: National Security long-term Insights Briefing* (online, October 2022) at 3.

589 Public Service Act 2020, Schedule 6, s 8.

590 Royal Commission report at part 8, chapter 4.8 at [34].

591 For example, the Canadian Security Intelligence Service (CSIS) publishes in its annual report a fulsome explanation of the threat environment in Canada: Canadian Security Intelligence Service *Public Report 2020* (online, April 2021) and Canadian Security Intelligence Service *Public Report 2021* (online, March 2022).

592 Cullen/Reddy report at 146.

Threat disruption: New Zealand Security Intelligence Service

11.24. The NZSIS has the function of collecting and analysing intelligence, and of providing that intelligence and analysis to persons, including those authorised by the responsible Minister.[593] Certain intelligence can be valuable if it is used to mitigate, reduce or otherwise disrupt a threat to national security. The NZSIS's annual reports for 2020 and 2021 raise two case studies that highlight the potential of threat disruption activity:

> 2020: Case Study 1: NZSIS has been conducting an investigation into a New Zealand citizen who is assessed to be working on behalf of a foreign state's intelligence services. The New Zealander is almost certainly collecting intelligence against New Zealand-based people who are viewed as dissidents by the foreign state's government. The target of our investigation uses overt and covert means to collect identifying information about these individuals and pass it to the foreign state's embassy in New Zealand.[594]
>
> 2021: Case Study 1: The NZSIS has been conducting an investigation into a New Zealand-based individual who sought to facilitate the transfer of sensitive New Zealand technologies and intellectual property to a foreign state. The New Zealander, who had long-term relationships with individuals linked to a foreign state's military and intelligence services, facilitated access to New Zealand persons and information through legitimate business dealings. The industries and technologies involved would highly likely benefit the foreign state's military capabilities.[595]

11.25. The NZSIS may currently issue warnings where, for example, an NZSIS officer identifies themselves in that capacity to a member of the public and makes a statement to that person that is intended to deter or dissuade them from undertaking activities that are a threat to New Zealand's national security. While authorised warnings fall within the functions of the NZSIS under the ISA, a lack of clarity exists as to how far such threat disruption activities might extend. The prohibition on law enforcement was the subject of two reports by the Inspector-General on warnings issued by the NZSIS.[596] This includes a recent report that reviewed a particular warning given by the NZSIS.[597]

Warnings and the limitations arising from the prohibition on 'law enforcement'

11.26. The activities of the NZSIS are limited by s 16 of the ISA, which provides that it is not the function of an intelligence and security agency to "enforce measures for national security".[598] An important issue relating to warnings is determining what comprises 'enforcement'. In the Inspector-General's view, the NZSIS may seek to influence the behaviour of individuals by giving advice or warning them of possible consequences from their behaviour. However, there are limitations on the way such warnings are expressed, which include the need to avoid any

---

593 Intelligence and Security Act 2017, s 10.

594 New Zealand Security Intelligence Service *2020 Annual Report* (2020) at 19.

595 New Zealand Security Intelligence Service 2021 *Annual Report* (2021) at 36.

596 Inspector-General of Intelligence and Security *Legality and propriety of warnings given by the New Zealand Security Intelligence Service* (online, 13 December 2017).

597 Inspector-General of Intelligence and Security *Review of an NZSIS Warning* (online, 18 October 2022).

598 This applies except in limited circumstances that are not applicable to the question of NZSIS threat disruption activities.

misapprehension about the powers of the NZSIS and to express advice in clear terms.[599] The ministerial policy statement "Collecting human intelligence" contains guidance on the issuing of warnings, which includes the caution that employees must take care to ensure a warning does not constitute enforcement action.[600] For example, it should be made clear to the individual being warned that they are not being detained or prosecuted by the NZSIS.

11.27. As recognised by the Inspector-General, a fine line exists between permitted warnings and unlawful enforcement activities. The prohibition on 'enforcing measures' for national security creates uncertainty over the scope of permitted warnings. It excludes more active threat disruption activities. Some potential threat disruption activities, for example, might include: using covert influence to discourage an individual from accessing online extremist groups; discrediting online extremist publications to prevent their spread; intervening with an individual or an individual's family to reduce a threat to national security and to provide an opportunity for an individual to receive support; or indicating knowledge of state-led interference operations without publicity harming diplomatic relations.

11.28. Threat disruption activities are used in other countries. For example, as part of its anti-terrorism legislation, the Canadian Security Intelligence Service (CSIS) obtained an explicit threat disruption function in 2015. This was clarified and expanded, after the entry into force in 2019 of the National Security Act (2017). Threat disruption activities that are otherwise unlawful, require judicial approval; lawful threat disruption does not. All threat disruption activities must reach a high threshold,[601] meet certain safeguards, be reported annually and are subject to oversight. The CSIS Act specifies that "for greater certainty", nothing in provisions setting out threat disruption powers "confers on the Service any law enforcement power".[602]

Should the New Zealand Security Intelligence Service have an explicit threat disruption function?

11.29. The question is whether there is benefit in including threat disruption as an explicit statutory function in the ISA. This would expand the tools available to the government to reduce threats to national security and seek to address them before they occur. An express mandate would provide clarity around the lawful scope of the NZSIS's threat reduction activities and provide greater transparency for the public. It may help to serve the public interest in the mitigation of such threats.

11.30. On the other hand, constraints would need to be placed on any threat disruption activities. The Inspector-General's report into NZSIS warnings highlights the difficulties that warnings may bring, particularly their effect on the due process and other rights of the individuals concerned.[603] Without constraints, warnings or any other threat disruption activities may be inappropriately used.

---

599 Inspector-General of Intelligence and Security *Legality and propriety of warnings given by the New Zealand Security Intelligence Service* (online, 13 December 2017) at [31.2] and [33]–[39].

600 Minister Responsible for the GCSB and NZSIS *Ministerial Policy Statement on Collecting Human Intelligence* (online, 1 March 2022) at [32].

601 There must be reasonable grounds to believe a particular activity constitutes a threat to the security of Canada, before the CSIS can take measures to reduce the threat. See Canadian Security Intelligence Service Act RSC 1985 c C-23, s 12.1(1).

602 Canadian Security Intelligence Service Act RSC 1985 c C-23, s 12.4.

603 Inspector-General of Intelligence and Security *Legality and propriety of warnings given by the New Zealand Security Intelligence Service* (online, 13 December 2017).

11.31. The Canadian National Security and Intelligence Review Agency undertook a review of the threat disruption powers of the CSIS in 2020 after five years' operation.[604] The review agency found that most measures taken satisfied the legal requirements under the CSIS Act and ministerial directions. Notably, **no** judicial warrant to authorise threat disruption activities involving unlawful activities had been sought over the five-year period. The report demonstrates the value of independent oversight of such a function. It also highlights the complexity of a threat disruption function and the need to have a robust framework for the exercise of such powers.

What might a threat disruption function look like?

11.32. It has been suggested by the NZSIS that the ISA could set out a specific threat disruption function for the NZSIS similar to the way in which the CSIS threat reduction function is articulated. Such a framework could permit the NZSIS to take lawful measures to reduce threats and enable it to carry out activities to reduce threats that would otherwise be unlawful under an authorisation. The NZSIS suggested the framework for undertaking lawful threat disruption activities should be placed in a ministerial policy statement. It also suggested that activity carried out in performance of this function would be subject to limitations, safeguards and oversight.

Is this an appropriate approach?

11.33. NZSIS already undertakes warnings and other activities that could be described as lawful threat disruption measures within its existing functions. The issue faced by the NZSIS is the lack of clarity around the scope of its existing powers concerning such activities and the lack of transparency from not having any explicit reference in the ISA. Section 16 of the ISA also restricts the NZSIS's ability to undertake more robust threat disruption activities that may tend towards enforcement action.

11.34. We see some merit in clarifying the NZSIS's threat disruption powers. However, a question is whether sufficient policy work has been undertaken to conclude that a specific threat disruption power, beyond warnings, should be included in the ISA. Leaving the detailed implementation to be set out in policy and procedures, especially if they are internal and not public, raises similar issues over the lack of transparency as encountered elsewhere in the ISA.

11.35. An issue also exists over threat disruption activities that would otherwise be unlawful. Should the NZSIS be authorised to undertake any kind of unlawful threat disruption activities? Where would the line be drawn between unlawful activities, such as leaking information where that might engage computer access offences in the Crimes Act 1961, and other unlawful activities, such as coercion? Is there sufficient social licence to give the NZSIS such powers, even with an authorisation? That the CSIS has had this power for five years, but not sought its use, suggests caution should be exercised over the necessity of authorising otherwise unlawful threat disruption activities, as distinct from lawful threat disruption activities.

11.36. A more appropriate approach would be to address warnings explicitly in the ISA and include an exception to s 16 to enable warnings to be issued to mitigate threats. We prefer this approach as ensuring greater transparency for the public over the role of the NZSIS in issuing warnings, as suggested by the Inspector-General in his latest report on warnings.[605] The Inspector-General

[604] National Security and Intelligence Review Agency *Review of CSIS Threat Reduction Activities: Review 2020–05* (online, 24 November 2021).

[605] Inspector General of Intelligence and Security *Review of an NZSIS Warning* (online, 18 October 2022) at [79]–[80].

also raised the potential for exploring an authorising framework for threat disruption that could enable more effective oversight of such activities, were the government and Parliament to consider that the scope for 'disruption' should be expanded or clarified.[606]

11.37. The review therefore recommends the ISA be amended to address warnings explicitly and include an exception to s 16 to enable warnings to be issued to mitigate threats. Further policy work should be undertaken to determine a possible new function of threat disruption activities that go beyond warnings. However, the review is not convinced of the merit in providing the NZSIS with a threat disruption power that extends to otherwise unlawful activities.

RECOMMENDATION 26

Amend the Intelligence and Security Act 2017 to explicitly include the ability for the New Zealand Security Intelligence Service to issue warnings to mitigate threats to national security and make an appropriate amendment to section 16 (Functions of intelligence and security agencies do not include enforcement).

Threat disruption: Government Communications Security Bureau

11.38. The information assurance and cyber-security functions of the GCSB include in s 12(1)(b):

> … doing everything that is necessary or desirable to protect the security and integrity of communications and information infrastructures of importance to the Government of New Zealand, including identifying and responding to threats or potential threats to those communications and information infrastructures.

11.39. The GCSB's information assurance and cyber-security activities are excluded from the prohibition on law enforcement activities in s 16 of the ISA. The GCSB can therefore seek authorisations under s 67(2) of the ISA to protect the security and integrity of communications and information infrastructures of importance to the government of New Zealand, including responding to threats or potential threats to those communications or infrastructures. This should enable a reasonably wide range of activities consistent with the GCSB's information assurance and cyber-security mandate to protect communications and information infrastructure. Hypothetical examples might include removing malware from communications infrastructure, stopping users from visiting websites that would infect their computers with malware, and blocking the downloading of malware associated with ransomware attacks.

11.40. The National Cyber Security Centre (NCSC – part of GCSB) works under the GSCB's mandate to help detect, deter and disrupt malicious activity in cyberspace. In 2020/21, NCSC disrupted over 2,000 malicious cyber events as part of the early phase of its Malware Free Networks (MFN) programme.[607] The review was advised this number reached 122,000 as of 30 June 2022. The NCSC is scaling-up the availability of MFN to make the service available to as many organisations

[606] Above n, at [83].
[607] National Cyber Security Centre *Cyber Threat Report 2020/21* (online, 16 November 2021) at 3.

as possible. Over time, it is expected that MFN will block more malicious traffic and provide insights and intelligence in support of increased detection.[608]

11.41. However, this part of the GCSB's legal mandate is limited to activity to protect communications and information infrastructures of importance to New Zealand.[609] The ISA does not enable the GCSB to take action to mitigate, disrupt or respond to threats outside of that cyber-security context, such as for counterterrorism purposes.

11.42. Malicious actors, including organised criminal and terrorist groups, are increasingly using cyber capabilities to carry out their activities. This trend is likely to increase, both in terms of the sophistication of the methods used and their boldness. Such activity includes: stealing sensitive commercial or government information; disrupting critical service providers and supply chains; disinformation and misinformation campaigns; foreign interference; theft of personal information for profit; and radicalising individuals to violence.

11.43. In this environment, it appears the GCSB lacks the necessary legislative tools to take measures that fall outside its information assurance and cyber-security mandate. Such measures could be aimed at cyber threat disruption and threat mitigation, including to protect New Zealand against threats from terrorism, violent extremism, foreign interference and transnational crime.

11.44. This lack of mandate can be contrasted with that of New Zealand's Five Eyes partners, which have spoken publicly about the use of cyber threat disruption activities outside of a cyber-security context, such as in the counterterrorism and transnational organised crime contexts. Although publicly available information is scant on the operational extent of these efforts, such activities are variously referred to as 'defensive' cyber operations,[610] 'offensive' cyber operations,[611] or 'deterrence' operations.[612]

11.45. Whether it is appropriate for the GCSB to have a broader mandate, beyond cyber security, to help mitigate malicious activity through cyberspace is a broad and complex policy question. Consideration would be needed of issues such as the scope of any such regime, the appropriate authorisation regime and oversight mechanisms. International legal considerations would also need to be taken into account concerning the use of offensive cyber operations. It would also be necessary to ensure coordination across the national security system, if consideration were to be given to whether the GCSB could use any additional powers to help other agencies, such as the Police and New Zealand Defence Force. The review considers that, in principle, there is a case to permit the GCSB to undertake cyber threat disruption activities outside the cyber-security context. However, detailed policy work is needed before any proposal would be ripe for further consideration.

---

608 Above n, at 9.

609 Section 13 of the ISA enables the intelligence and security agencies to help the New Zealand Police and New Zealand Defence Force for the purposes of facilitating the performance or exercise of their functions, duties or powers. If these agencies were mandated to carry out such activities, GCSB could therefore help them, if requested.

610 For example, the United States of America works with partner countries in the 'Hunt Forward Operations' where cyber operators sit side-by-side with the partner and 'hunt' on the networks of the host nation's choosing, looking for malicious cyber activity and vulnerabilities: United States Cyber Command, Public Affairs "U.S. conducts first Hunt Forward Operation in Lithuania" (4 May 2022) <cybercom.mil>.

611 Tom Uren, Bart Hogeveen and Fergus Hanson *Defining offensive cyber capabilities* (Australian Strategic Policy Institute, 4 July 2018).

612 United States Cyber Command "Posture statement of Gen. Paul M. Nakasone, commander, U.S. Cyber Command before the 117th Congress" (5 April 2022) <cybercom.mil>.

RECOMMENDATION 27

The Government should undertake further policy work as a priority to determine whether the Intelligence and Security Act 2017 should be amended to include ability for the Government Communications Security Bureau and/or the New Zealand Security Intelligence Service to undertake threat disruption activities (beyond giving warnings), including cyber threat disruption activities. This would need to consider the scope of any such regime, whether it should include otherwise unlawful threat mitigation activities, the appropriate authorisation regime, limits, safeguards and oversight mechanisms.

Use of vetting information

11.46. As part of its protective security service, the NZSIS undertakes security vetting of individuals who are required to access classified information for their work. The higher the security clearance level the greater the scrutiny of the individual's suitability to hold a clearance. The information must be provided by candidates and is necessarily of a wide-ranging and extremely sensitive nature that candidates would ordinarily have no reason to disclose. This includes highly personal information relating to, among other things, sexuality, social habits, physical and mental health, financial well-being, and personal information about a candidate's family members and referees. It may reveal information about potential alcohol and drug dependency.[613]

11.47. To provide the candidates and referees with the confidence to be candid and forthcoming with such information, vetting information must be attended by appropriate safeguards. This is particularly because information obtained during the vetting process is not limited to the candidate but includes personal information about their family members, friends, referees and other associates. Section 220 of the ISA restricts the use of information obtained by the NZSIS during a security clearance assessment process. It may only be used for the purposes of the security clearance assessment, any other security clearance assessment, or counter-intelligence. For the purposes of this section, counter-intelligence means the intelligence activities carried out to identify and counteract the threat, or potential threat, of unauthorised disclosure of official information by a person who holds, or has held, a New Zealand government-sponsored national security clearance. This provision overrides information privacy principle 10 (use of personal information for a secondary purpose) in s 22 of the Privacy Act 2020.

11.48. The Inspector-General's annual report for 2020/21 outlines an instance in the reporting year where the NZSIS shared information about potential criminal offending with the Police.[614] However, s 220 does not permit the use of vetting information unless it is for a security clearance assessment or counter-intelligence purpose. This means the NZSIS is unable to share information for law enforcement purposes, even in relation to serious criminal offending or where an imminent threat may exist to the safety or life of a person.

11.49. The security vetting process necessarily relies on the free and frank sharing of information by candidates and their referees. While the security vetting process involves the collation and

[613] See Inspector-General of Intelligence and Security *Review of NZSIS holding and use of, and access to, information collected for security vetting purposes* (online, 7 April 2016) at [8.2] and [36.1].

[614] Inspector-General of Intelligence and Security *Annual Report for the year 1 July 2020 to 30 June 2021* (online, 11 November 2021) at 5.

assessment of information from various sources, some information will be uniquely within the knowledge of the candidate or their referees. It is possible that, if candidates and referees were aware such information could be disclosed to Police for enforcement action, this would have a negative impact on their sharing it. This could have a similar effect for candidates' referees.

11.50. A question has arisen as to whether vetting information may be released where an imminent threat of harm exists in order to prevent that harm. Although the number of cases where this may arise is likely to be small, the impact is potentially large. Where an Agency is aware of an imminent threat to the life or health of an individual, arguably they have a duty to act to prevent that threat. This suggests it may be appropriate to include a narrow exception to s 220 where a serious threat exists to the life or health of an individual. This would balance the need to protect individuals from harm, while maintaining the integrity of the vetting process.

11.51. A narrow exception is consistent with the approach taken in other situations where a public interest exists in ensuring the continued provision of information within specific contexts and relationships. Rule 8.2 in the Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008 requires a lawyer to disclose information where he or she "reasonably believes that disclosure is necessary to prevent a serious risk to the health or safety of any person". Rule 10(1)(d) of the Health Information Privacy Code 2020 permits a health agency to use information obtained for one purpose for another purpose, if the agency believes on reasonable grounds this is necessary to prevent or lessen a serious threat to "public health or safety; or the life or health of the individual concerned or another individual".

11.52. We recommend that a limited exception be included in s 220 to enable disclosure of vetting information where there are reasonable grounds to believe there is a serious threat to the health or safety of any person and the proposed disclosure would prevent or lessen that threat. To ensure adequate safeguards, decisions to make such disclosure should require Director-General approval. A requirement should also be in place to notify the Inspector-General as soon as practicable after the disclosure and to report the number of times this is relied on in the NZSIS's annual report, and whether disclosure was to the Police or another entity.

RECOMMENDATION **28**

Amend section 220 (Use of information provided for security assessment clearance) of the Intelligence and Security Act 2017 to include an exception to enable the disclosure of vetting information where the Director-General considers that there are reasonable grounds to believe there is a serious threat to the health or safety of any person and the proposed disclosure would prevent or lessen that threat; and require reporting to the responsible Minister and the Inspector-General of Intelligence and Security in the event of any such disclosure.

SECTION

05

Safeguards – independent control, oversight, accountability and transparency

CHAPTER 12
Oversight: Recommended changes

Introduction

12.1. In this chapter, we set out our recommendations in relation to the three principal oversight mechanisms under the Intelligence and Security Act 2017 (ISA): the Intelligence and Security Committee, the Inspector-General of Intelligence and Security (Inspector-General) and the Commissioners of Intelligence Warrants (the Commissioners).[615] Before we do so, however, we should make three points.

12.2. First, the three oversight mechanisms discussed in this chapter are part of a wider scheme of constraints that govern the activities of the intelligence and security agencies (the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) and referred to in our report as 'the Agencies'), as discussed in chapter 4. Each of the three oversight mechanisms is important, but they operate within a legislative framework that seeks to constrain what the Agencies do in a variety of other ways, including functions performed by the Minister responsible for each of the Agencies.

12.3. We also made the point in chapter 4 that the oversight mechanisms discussed in this chapter operate in different ways. The Commissioners operate as controls, in the sense that before the Agencies are entitled to undertake certain activities, they must obtain a warrant or other authorisation from a Commissioner (as well as the Minister). Where a Commissioner grants or rejects a warrant application, or imposes conditions on a warrant, that determines what the Agency may do and how they may do it. By contrast, the Inspector-General generally performs a review function, examining issues of legality and propriety on a predominantly 'after-the-event' basis.[616] Of course, in performing that review function, the Inspector-General may well seek to influence the Agencies' behaviour in the future.

12.4. Second, we undertake this discussion against the background that, in chapter 4, we identified a gap in the scope of the oversight arrangements established under the ISA. The ISA refers to "facilitating effective democratic oversight" in its purpose section and in its description of the duties of the Agencies.[617] We accept that providing effective democratic oversight is a multi-layered enterprise, in the sense that the various oversight mechanisms established by the ISA

---

[615] As discussed in chapter 4, the Minister responsible for each of the Agencies also provides important guidance to them through, for example, issuing Ministerial Policy Statements, considering warrant applications, participating in the setting of priorities and in performing other functions under the ISA. In this chapter, we are discussing the quasi-judicial, independent and parliamentary oversight described in chapter 4.

[616] This role also contributes to revisions of Ministerial Policy Statements and Direct Access Agreements.

[617] Intelligence and Security Act 2017, ss 3 and 17 respectively.

are all intended to contribute to ensuring that objective – Commissioners bring an independent, judicial assessment to whether the requirements for the issue of warrants are met, thereby fostering public confidence in the Agencies' exercise of intrusive powers; the Inspector-General provides an independent expert assessment of the legality and propriety of the Agencies' actions and addresses individual complaints, and in those ways fosters public confidence in the Agencies; but, in principle at least, the Intelligence and Security Committee has, as a committee of parliamentarians, the greatest potential for ensuring truly democratic oversight.

12.5. The gap, as we see it, is that presently there is no independent examination of the effectiveness of the Agencies in meeting a fundamental purpose of the ISA, which is that they contribute effectively to the protection of New Zealand's national security, to its international relations and to its economic and other interests; yet the reason that we give the Agencies intrusive powers and allow them to operate in secret is because we want them to be effective – we want them to contribute to our protection and to help us to make our way in a challenging world.

12.6. We should make it clear, however, that while we regard this gap as a significant one, it is not the only reason that we recommend enhancements designed to achieve effective democratic oversight of the Agencies in the discussion that follows.

12.7. Third, the issues relating to workarounds and inconsistencies identified in chapter 3 are relevant in the context of oversight. The ISA sets out constraints and establishes oversight mechanisms for the Agencies, reflecting that they operate largely in secret and can exercise intrusive powers; yet other government agencies also undertake similar intelligence collection and analysis activities free of the types of constraints and oversight that apply to the Agencies. As noted in chapter 3, this raises issues of legislative consistency and coherence. While these are not issues that we will discuss in any detail, they do have some relevance in the context of oversight, given developments in comparable countries and in light of some of the observations of the Royal Commission of Inquiry.

Intelligence and Security Committee

12.8. We referred in chapter 1 to the 'democratic paradox', the idea that democracies set up intelligence and security agencies to protect their safety, their democratic institutions and their open and free way of life but then fear the agencies they have established because they necessarily operate largely in secret and have intrusive powers that may affect fundamental freedoms. As we emphasised in chapter 4, the ISA's purpose is to protect New Zealand as a free, open and democratic society by (among other things) "ensuring that the powers of the intelligence and security agencies are subject to institutional oversight and appropriate safeguards".[618] The overall purpose of the oversight provisions in Part 6 of the ISA is to "provide for the independent oversight of [the Agencies] to ensure that [the Agencies] act with propriety and operate lawfully and effectively".[619] Apart from being essential to ensuring that intelligence and security agencies are doing their job in accordance with their powers, effective oversight mechanisms are an important means for assisting intelligence and security agencies in democracies to gain and retain social licence, which is particularly important in an increasingly multicultural and diverse country such as New Zealand.

[618] Section 3.
[619] Section 156(1).

12.9. We have concluded that the Intelligence and Security Committee (the Committee) as presently constituted is not capable of performing the type of independent oversight of the Agencies that should occur in a democracy. In saying this, we are not being critical of the members of the Committee, whether past or present. We acknowledge that the former Chair of the Committee, Rt Hon Jacinda Ardern, has enhanced the role of the Committee by scheduling more frequent meetings covering a range of topical national security issues and has facilitated the provision of classified information to the Committee. We were able to attend one of the Committee's meetings and felt it provided an environment in which senior members of the government, Opposition and other parties could discuss issues of significance to New Zealand's national security in a secure environment, free of the pressures of party politics. Undoubtedly, that is beneficial in a democracy. The Committee provides an opportunity for engagement that the Directors-General value – from their perspective, it provides a useful opportunity to brief senior government and political leaders on shared areas of concern related to national security.

12.10. However, given the comments made about the Committee during the parliamentary debates on intelligence and security legislation over the years, our interviews with past and present members of the Committee and with Inspectors-General and Deputy Inspectors-General, submissions from interested stakeholder groups, including Kāpuia, academics and legal experts, the experience of similar committees in comparable jurisdictions and our own consideration of the constitutional and other interests engaged, we believe that the Committee does not and cannot operate as an effective means of independent democratic oversight of the Agencies. As one submitter put it:

> The Intelligence and Security Committee is the only one of the three major oversight bodies of New Zealand's intelligence and security agencies in a position to provide a democratic check on the actions of the agencies, and on the decisions of the Minister in approving highly intrusive surveillance, but it is also the only one that is statutorily barred from knowing what New Zealand's security agencies are actually doing. This is a problem that needs to be addressed.[620]

12.11. We will explain our conclusion under three headings: background, overseas experience and the case for change. We will then set out what we recommend and will attempt to respond to some of the objections that have been raised to our views during the consultative process.

Background

12.12. It is useful to recall the reasons that the Committee was established in the first place in 1996. As described in chapter 4, the government's objective was to increase the oversight and accountability of the Agencies by doing what comparable jurisdictions had done, namely establishing a parliamentary oversight committee. The need for such oversight was accepted by both major parties and the intent was, according to the then Prime Minister Rt Hon Jim Bolger, for a committee to "perform the functions [of parliamentary and administrative] oversight … that in the case of other government departments are performed by Select Committees".[621] It was envisaged that the Committee would comprise the Prime Minister, Leader of the

[620] As we understand it, the reference in the quote to the statutory bar on knowing what the Agencies are actually doing is a reference to s 193(2)(b), which provides that it is not one of the Committee's functions to inquire into "any matter that is operationally sensitive, including any matter that relates to intelligence collection and production methods, or sources of information".

[621] Hansard 1995, 10780.

Opposition and other senior members of Parliament, meeting in secret to "receive sensitive information, deal with it appropriately and to respond in whatever manner was deemed correct at that time".[622] Although intended to perform the types of function that select committees perform, the Committee was and remains a statutory committee, not a select committee. Accordingly, it differs from select committees in some respects, most notably that the Prime Minister and other members of the Executive are members of it.

12.13. Given that the objective was that the Committee would perform the functions in respect of the Agencies that select committees performed for other departments, it is useful to note what the functions of select committees are. A key function is to hold the Executive to account.[623] There are several contexts in which select committees do this – through their scrutiny of proposed legislation, during budget processes, through financial and performance reviews of government entities, where they ask for briefings and where they hold inquiries. Reflecting the key function of holding the Executive to account, members of the Executive are, by convention, not members of subject select committees.[624] Obviously, in performing the various tasks just mentioned, select committees perform functions besides holding the Executive to account, such as assisting Parliament to improve the quality of the legislation it enacts.

12.14. The Committee has not had an active role in oversight in the way a select committee normally would have. While New Zealand's select committees generally meet weekly when Parliament is sitting, the Committee has met only three or four times a year, at least until 2022 when it began to meet more often.[625] Former members of the Committee told us that while the Committee dealt with 'pay and rations' issues satisfactorily, it was not effective in other respects – it did not receive competing streams of advice on intelligence and security issues but rather relied on what it was told by the Agencies; it had no capacity to undertake significant investigative or other work; it did not consider the effectiveness of the Agencies. The Committee has not carried out inquiries or produced reports (apart from anodyne annual reports).

12.15. In terms of considering legislation, the Committee did consider the draft New Zealand Intelligence and Security Bill in 2016 in a preliminary way, but it has not considered other relevant legislation. Counter-terrorism legislation and other national security matters have been referred to other committees without an opportunity for consideration by the Committee. For example, in 2019, the heads of the Agencies appeared before the Justice Select Committee when it held an inquiry into foreign interference in the 2017 general election and the 2016 local elections, and, unlike in other jurisdictions, the inquiry did not access classified information.[626] All in all, it seems doubtful that this was what the government had in mind when the Committee was established in 1996, but even if it was, we consider it is time to enhance the Committee's role.

12.16. It is not clear to us whether, and if so to what extent, the structure and operation of Committee has ever been reviewed. There is no discussion of alternative models in the Cullen/Reddy report, although their report did recommend that the government "keep [the structure of the Committee] under consideration in future reviews".[627] It also included some recommendations

---

[622] Hansard 1996, 13331.

[623] See Mathew Palmer and Dean Knight *The Constitution of New Zealand: A Contextual Analysis* (Hart Publishing, 2022) at 123–124 for a concise description of the functions of subject select committees.

[624] Above n, at 112. There are some exceptions to this, such as the Privileges Committee.

[625] The Committee held seven meetings in 2022, and a further one was cancelled as a result of the death of Queen Elizabeth.

[626] See Laura Walters "Foreign interference inquiry 'becoming a farce'" Newsroom (online, New Zealand, 9 August 2019) and Rebecca Kitteridge, Director-General of Security, and Andrew Hampton, Director-General of GCSB, "Directors-General submission to the Justice Select Committee Inquiry into 2017 General Election and 2016 Local Elections".

[13] Cullen/Reddy report at 71.

relevant to the independence of the Committee, specifically, an increase in its maximum size and provision for the chairperson to be elected by the Committee (rather than legislation designating the Prime Minister to be the Chair). In addition, the report recommended extending the Committee's functions to cover the National Assessments Bureau, including an annual financial review of the Bureau's performance, and proposed that the Committee be able to request that the Inspector-General undertake certain inquiries. In the ISA, Parliament did increase the size of the Committee from five to a maximum of seven members and gave the Committee the ability to request an inquiry by the Inspector-General, but it did not widen the Committee's remit to incorporate the National Assessments Bureau or provide for the Chair to be elected by the Committee.

12.17. Finally in this context, we note that the Royal Commission of Inquiry made several recommendations relevant to the work of the Committee, the most important being that the government:[628]

> strengthen the Parliamentary Intelligence and Security Committee so that it can provide better and informed cross-Parliamentary oversight of the national security system (including the counter-terrorism effort) and priority-setting, and members can access sensitive information as necessary for such oversight.

Overseas experience

12.18. We do not propose to examine the equivalents of the Committee in other comparable countries in any detail. We will focus on the Five Eyes countries (other than the United States, which has its own peculiarities).

12.19. There are several publicly available comparisons of the oversight arrangements in the Five Eyes countries. They are useful sources of information, although care is needed to check that the information in them is fully up to date.[629] Our purpose in referring to these parliamentary oversight arrangements is partly because the government referred to them as a justification for the establishment of Intelligence and Security Committee in 1996 and partly because they are, in any event, useful comparators.

12.20. Before we summarise the overseas experience, however, we should acknowledge a point made by Jonathan Boston, David Bagnall and Anna Barry in their recent work on parliamentary scrutiny:[630]

> Caution is needed in assessing the relevance of overseas models and practices for New Zealand. After all, parliamentary democracies differ, often markedly, with respect to their constitutional, political, institutional and administrative systems. Hence, mechanisms that are effective in one jurisdiction may not be similarly effective elsewhere … New Zealand is a highly centralised, unitary state with a relatively small unicameral legislature and highly disciplined parliamentary parties. These aspects of our constitutional

---

[628] Royal Commission of Inquiry *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) (*Royal Commission report*), recommendation 6.

[629] Bill Browne *Parliamentary oversight of intelligence agencies* (Australian Institute, Discussion Paper, September 2020); Andrew Defty "From committees of parliamentarians to parliamentary committees: comparing intelligence oversight reform in Australia, Canada, New Zealand and the UK" (2020) 35(3) Intelligence and National Security 367; Parliamentary Library Research Paper *Oversight of Intelligence Agencies: A Comparison of the 'Five Eyes' Nations* December 2017.

[630] Jonathan Boston, David Bagnall and Anna Barry *Foresight, insight and oversight: Enhancing long-term governance through better parliamentary scrutiny* (Institute for Governance and Policy Studies, Victoria University of Wellington, June 2019) at 114.

framework and political culture are likely to impede reform options that depend, for instance, on an upper house or a legislative chamber with an abundance of backbench members of Parliament (MPs).

We bear this in mind in the discussion that follows.

12.21. Since the Committee was established in 1996, other comparable countries have increased their expectations of their equivalent committees and have enhanced their powers accordingly. In other Five Eyes countries, the jurisdiction of the equivalent committees has been extended to cover other elements of the national security and intelligence community, such as the strategic defence intelligence assessment function, geospatial intelligence agencies and the central intelligence assessment function.[631] In Canada and the United Kingdom (UK) in particular, the equivalent committees have been given greater powers and additional staff. Both conduct inquiries and produce public reports that deal with a wide range of matters, although subject to some redactions, these reports are informative and relatively detailed.[632]

12.22. Even with these reforms, however, there remains a concern in both jurisdictions that the Executive, through the Prime Minister, has the ability to exercise too much control over the work and output of the committees.[633] For example:

- In Canada, the members of the committee are appointed by the Governor in Council on the advice of the Prime Minister, as is the Chair. While the Prime Minister has certain consultation obligations, Parliament as an institution has no statutory role to play in the appointment process. In New Zealand, the United Kingdom and Australia, Parliament does have a role.
- In the UK, although the Prime Minister's powers have been diminished in some respects,[634] they can effectively delay the publication of potentially embarrassing reports by the committee, as appears to have occurred in relation to the publication of the committee's report on Russian interference.[635]
- The process for the appointment of a new committee following a general election has also been criticised in the UK. Following the December 2019 election, the committee was not reconstituted until 14 July 2020, some eight months after the former committee had vacated their posts on the dissolution of Parliament in November 2019. The allegation was that this delay related, in part at least, to the Russia report, just referred to, which could not be released until there was a committee in place.[636] The Canadian legislation attempts to

[631] In New Zealand's context, New Zealand Defence Intelligence within the NZDF and the National Assessments Bureau within DPMC, among others.

[632] For the relevant legislation and background to these developments, see, for the United Kingdom, the Justice and Security Act 2013 (UK) and *Justice and Security Green Paper* (October 2011); for Canada, National Security and Intelligence Committee of Parliamentarians Act SC 2017, c 15 and *Security, Freedom and the Complex Terrorist Threat: Positive Steps Ahead – Interim Report of the Special Senate Committee on Anti-terrorism* (March 2011), which stated (at 44) "Canada now lags significantly behind its allies on the issue of parliamentary oversight as the only country that lacks a parliamentary committee with substantial powers of review over matters of national security."

[633] See, for example, "Intelligence and security committee report signed off after complaint to PM" *The Guardian* (online, United Kingdom, 24 November 2021).

[634] For example, the Prime Minister no longer appoints the Chair and members of the Committee. Rather, the Prime Minister nominates members, but they are appointed by the House from which they are drawn; the Chair is chosen by the members of the Committee.

[635] United Kingdom's Intelligence and Security of Parliament "Intelligence and Security Committee of Parliament publish predecessor's Russia Report" (press release, 21 July 2020).

[636] See, for example, Andrew Defty "Where is the Intelligence and Security Committee and why does its absence matter?" (9 June 2020) Hansard Society <www.hansardsociety.org.uk>.

deal with this by requiring that the committee be appointed within 60 days of the day on which Parliament is summoned to sit following a general election;[637] in New Zealand, the Prime Minister must present to the House for endorsement the names that have been nominated for membership under the prescribed processes "as soon as practicable after the commencement of each Parliament".[638]

12.23. We have had the opportunity to discuss the UK committee with a former Chair, Rt Hon Dominic Grieve KC, and the Canadian committee with the current Chair, Hon David McGuinty PC and three members of the committee's staff. As a consequence (and despite the difficulties just mentioned), we have no doubt that they provide more effective democratic oversight than their New Zealand counterpart.

12.24. Relevant features of the Canadian and UK committees are:

- By statute, members of the Executive may not be members of either committee.[639] Rather, they are composed of non-Executive members of Parliament. In that sense, the committees are independent of the Executive.
- The members of both committees have independent access to classified material. In Canada, this is because the members of the committee must hold high-level clearances and must take a specified oath or affirmation;[640] in the UK, it is because committee members come within the ambit of Official Secrets Act 1989.
- Both committees are supported by their own secretariats of cleared staff, in each case about 10 staff.
- Both committees meet regularly and are, in a real sense, working committees. For example, in the period July 2019 to July 2021, the UK committee held 30 full committee meetings (including evidence sessions with government Ministers, senior officials from across the intelligence community and external experts), visited organisations within the intelligence community on five occasions, held bilateral discussions with the Canadian intelligence community and held 17 other meetings.[641]
- Both committees have jurisdiction to consider a wider range of matters in relation to intelligence and security agencies than is the case in New Zealand. For example, they can (subject to some limitations) inquire into operational matters such as intelligence collection and specified activities of other government agencies, which the New Zealand Committee cannot. As an illustration, one of the main functions of the UK committee is to "examine **or otherwise oversee** the expenditure, administration, policy **and operations**" of the agencies within the jurisdiction of the committee.[642] (The bolded language was added in 2013 to the language used in the original 1994 legislation, which was what prompted the government to set up the New Zealand Committee.)

---

637 National Security and Intelligence Committee of Parliamentarians Act SC 2017, c 15, s (1.1).

638 Intelligence and Security Act 2017, s 196(1). As DPMC has pointed out, the fact that there will be a pause in the Committee's operations until a new Committee is created after a general election creates some difficulty, but it is not clear how this could be resolved satisfactorily.

639 For Canada, see the National Security and Intelligence Committee of Parliamentarians Act SC 2017, c 15, s 4(1) and for the UK, see Justice and Security Act 2013 (UK), s 1(4).

640 National Security and Intelligence Committee of Parliamentarians Act SC 2017, c 15, s 10.

641 Intelligence and Security Committee of Parliament *Annual Report 2019-2021* (10 December 2021) at [6].

642 Justice and Security Act 2013 (UK), s 2(1). The limitations in respect of operational matters are set out in s 2(3) and (4).

- Both committees have jurisdiction in relation to a broader range of agencies with intelligence and security functions than is the case in New Zealand. Both, for example, have jurisdiction in relation to the equivalents of the National Assessments Bureau and certain activities of New Zealand Defence Intelligence.[643]
- Both committees conduct inquiries, issue substantive public reports on particular topics and (occasionally) hold public hearings, as well as publish annual reports.

12.25. To understand the work of these two committees, it is helpful to note a sample of their public reports. For example, the UK committee has, over the past few years, produced reports dealing with extreme right-wing terrorism, Russia, privacy and security, and diversity and inclusion in the UK intelligence community.[644] The Canadian committee has produced reports on matters such as the intelligence function of Canadian defence authorities as they affect Canadians,[645] the Canadian government's framework and activities to defend government systems from cyber-attack[646] and the national security and intelligence activities of Global Affairs Canada (the Canadian equivalent of the Ministry of Foreign Affairs and Trade).[647] These are in addition to their annual reports, which are significantly more detailed than the annual reports produced by New Zealand's Committee.[648]

12.26. The equivalent committee in Australia is the Parliamentary Joint Committee on Intelligence and Security. Initially, the committee's mandate related to only one intelligence and security agency. Since 2001, however, the committee's mandate has been expanded in stages to cover additional agencies so that now it covers the core intelligence and security agencies, defence intelligence and intelligence agencies with geospatial and intelligence assessment functions. The 2017 Independent Intelligence Review of the Australian national security and intelligence sector[649] recommended a further expansion of the committee's role to cover all 10 agencies that comprise Australia's national intelligence community. However, this was put on hold while a further review of the legal framework for the intelligence community was undertaken[650] and is currently under consideration by the Australian government.

---

643 In Canada, the equivalent Committee's mandate is not limited but defined in s 8(1)(b) of the National Security and Intelligence Committee of Parliamentarians Act SC 2017, c 15 as "any activity carried out by a department that relates to national security or intelligence, unless the activity is an ongoing operation and the appropriate Minister determines that the review would be injurious to national security".

644 Intelligence and Security Committee of Parliament *Extreme Right-Wing Terrorism* (13 July 2022); Intelligence and Security Committee of Parliament *Russia* (21 July 2020); Intelligence and Security Committee of Parliament *Privacy and Security: a modern and transparent legal framework* (12 March 2015). Intelligence and Security Committee of Parliament *Diversity and Inclusion in the UK Intelligence Community* (18 July 2018).

645 National Security and Intelligence Committee of Parliamentarians *Special Report on the Collection, Use, Retention, and Dissemination of Information on Canadians in the context of the Department of Defence and the Canadian Armed Forces Defence Intelligence Activities* (12 March 2020).

646 National Security and Intelligence Committee of Parliamentarians *Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack* (14 February 2022)

647 National Security and Intelligence Committee of Parliamentarians *Special Report on the National Security and Intelligence Activities of Global Affairs Canada* (27 June 2022).

648 See, for example, Intelligence and Security Committee *2020/21 Annual review of the New Zealand Security Intelligence Service* (March 2022), Intelligence and Security Committee 2020/21 *Annual review of the Government Communications Security Bureau* (March 2022).

649 Michael L'Estrange AO and Stephen Merchant PSM *2017 Independent Intelligence Review* (18 July 2017).

650 Dennis Richardson *Comprehensive Review of the Legal Framework of the National Intelligence Community* (December 2019).

12.27. Again, members of the Executive may not be members of the Parliamentary Joint Committee.[651] As just noted, the committee has broader jurisdiction than the New Zealand Committee in terms of the agencies it covers, but not as broad as that of the Canadian and UK committees.[652] It has a long list of functions, but broadly, they relate to providing oversight of Australian intelligence agencies by reviewing their administration and expenditure, conducting statutory reviews of certain legislation and reviewing national security bills introduced into Parliament. The committee's workload in the last Parliament was significant – it undertook 44 reviews and inquiries and tabled reports in relation to 38 of these; it also presented advisory reports on 12 Bills. Members have access to classified information without the need to obtain a clearance.

12.28. However, the structure and powers of the committee have been criticised: [653]

> Australia's parliamentary oversight of its intelligence community is weak compared to that of other countries within the Five Eyes. Most significantly, parliamentarians in the UK, USA and Canada have oversight over the operations and activities of the intelligence agencies, which Australia and New Zealand lack.

The case for change

12.29. As we have said, when New Zealand's Committee was established in 1996, the government drew on the experience of other countries. To the extent that equivalent committees in comparable jurisdictions provide a benchmark, New Zealand has fallen significantly behind. In addition to this, we found strong support among consultees and submitters for restructuring the Committee so as to expand the scope of its work, enhance its powers and increase its effectiveness as an oversight body. Indeed, this was one area where our inquiries produced an almost unanimous response.[654]

12.30. We consider that the Committee as presently constituted is lacking in three fundamental respects:

- independence from the Executive
- the capacity to undertake meaningful scrutiny of the work of the Agencies and in particular, their effectiveness
- the power to examine other agencies within the broader national security and intelligence community whose work raises similar issues to those raised by the work of the Agencies and whose work is relevant to the Agencies' effectiveness.

12.31. Notwithstanding the caution noted above, we believe change is required to achieve more effective democratic oversight of the Agencies (and, indeed, the intelligence community more generally). We note that this possibility was foreseen at the time the ISA was going through Parliament. When introducing the second reading debate, Hon Christopher Finlayson KC made the following prescient observation:[655]

---

[651] Intelligence Services Act 2001, 1st Schedule, cl 14(6).

[652] Dennis Richardson *Comprehensive Review of the Legal Framework of the National Intelligence Community – Volume 3: Information, Technology, Powers and Oversight* (December 2019).

[653] Bill Browne *Parliamentary oversight of intelligence agencies* (Discussion Paper, Australia Institute, 2 September 2020).

[654] We note in particular that the former Attorney-General and Minister responsible for the Agencies, Hon Christopher Finlayson KC, has argued that the Intelligence and Security Committee needs to be fundamentally reformed: see Christopher Finlayson *Yes, Minister* (Allen & Unwin, 2022) at 170–171.

[655] Hon Christopher Finlayson during the Second Reading of the New Zealand Intelligence and Security Bill (9 March 2017) 720 NZPD.

> I would say, of course, that this Bill is subject to a mandatory review clause. The Intelligence and Security Committee has evolved over the years since the concept was first introduced in 1996 and there could well be changes that future Parliaments may wish to introduce. But for the moment, as we develop this committee, I think we have made a very good start …

Later when the Bill was being considered in the Committee of the Whole, Mr Finlayson described the Committee as an evolving one and said there was a legitimate question as to whether the Minister in charge of the Agencies should be a member of it.[656]

12.32. We have considered whether the existing Committee structure could be retained but 'tweaked' in some way. We were conscious in this connection of the Prime Minister's efforts to expand the work of the Committee and increase the frequency of its meetings.

12.33. However, we do not see that as a viable option for two reasons. First, while the Committee's present structure may have been appropriate when the Committee was first established,[657] it is no longer fit for purpose as a matter of principle. The dominance of the Executive on the Committee cannot, in our view, be defended. Second, even if there was not that problem of principle, it would be impractical for the Committee as presently constituted to do what the Canadian and UK committees do and what we think the New Zealand Committee should do, given the other commitments of its members. The Prime Minister, other senior Ministers and the Leader of the Opposition do not have the time that would be needed to be a member of an intelligence and security committee that provides the type of oversight we envisage.

12.34. We will discuss the need for change to the Committee under two headings:

- Why is effective Parliamentary oversight important?
- What would an effective Intelligence and Security Committee look like?

Why is effective Parliamentary oversight important?

12.35. Given the extent of oversight provided through mechanisms such the Inspector-General of Intelligence and Security, the Commissioners of Intelligence Warrants and, to some extent, Ministers, we need to remind ourselves of why New Zealand needs effective parliamentary oversight of the country's security and intelligence functions.

12.36. The reason derives from our constitutional arrangements. The ISA speaks of "effective democratic oversight". The Cabinet Manual describes democracy as the "underlying principle" of New Zealand's constitutional arrangements.[658] Democratic elections produce Parliaments, from which the Prime Minster and Cabinet are drawn. As Matthew Palmer and Dean Knight put it:[659]

> Parliament stands at the centre of New Zealand's constitutional system and radiates the nation's strong commitment to representative democracy.

---

[656] Hon Christopher Finlayson during the Committee of the Whole House consideration of the Intelligence and Security Bill (16 March 2017) 720 NZPD.

[657] International experience indicates that initial efforts at Parliamentary oversight of intelligence and security agencies tended to be rather tentative and limited because such oversight was new and, no doubt, challenging for both agencies and governments. As experience and confidence has grown, however, Parliamentary oversight has tended to expand in scope and become more rigorous.

[658] Cabinet Office *Cabinet Manual* 2017 at 3.

[659] Matthew SR Palmer and Dean R Knight *The Constitution of New Zealand a Contextual Analysis* (Hart Publishing, October 2022) at chapter 4.

12.37. As the fundamental democratic institution in New Zealand's constitutional arrangements, Parliament has a responsibility to hold the Executive to account. It needs to have processes in place to ensure that public money is spent effectively, efficiently and appropriately. More than that, however, national security and intelligence activities raise important policy issues that go to the nation's essential values. These arise both generally and in specific contexts and require scrutiny through some form of parliamentary process. Effective democratic oversight is not simply important but imperative given:

- the significance of intelligence collection and analysis activities to the safety of the country, its institutions, its infrastructure, its communities and its people, and to objectives such as facilitating good decision-making within government
- the challenges that arise from intelligence and security agencies having to operate largely in secret and having the ability to act in ways that affect fundamental freedoms.

12.38. Because the Agencies exercise intrusive powers and operate largely in secret, special arrangements are required to provide meaningful parliamentary oversight. But this does not alter the basic point – that it is Parliament's responsibility, ultimately, to provide effective democratic oversight and input and to hold the Executive to account.

12.39. In the study mentioned at paragraph [12.20] above, Boston, Bagnall and Barry summarise the importance of parliamentary scrutiny as follows:[660]

> Parliamentary scrutiny of the Executive branch of government is fundamental for political accountability. It provides a crucial means for elected representatives to identify current and projected policy problems, poor decision-making processes, ineffective implementation and corrupt practices. It is equally vital in enabling members of Parliament (MPs) to examine whether a government is adequately safeguarding the interests of current and future citizens. Effective political accountability, in turn, is essential for building and maintaining public trust in the institutions of government and upholding the legitimacy of the democratic system. Robust accountability entails, among other things, the effective exercise of foresight, insight and oversight.

Although the focus of that study was on enhancing long-term governance, this statement has broader application. Namely, effective accountability requires transparency.

12.40. The democratic paradox to which we referred earlier means that accountability through Parliament should be an important tool for maintaining public confidence in the Agencies; but to achieve that, it must be seen as being effective. An enhanced Committee could meet the Royal Commission's recommendation that it promote transparency and public engagement. The Royal Commission recommended that:[661]

> require in legislation the Minister for National Security and Intelligence to publish during every parliamentary cycle the National Security and Intelligence Priorities and refer them to the Parliamentary Intelligence and Security Committee for consideration; the responsible minister publish an annual threatscape report; and the Parliamentary Intelligence and Security Committee to receive and consider submissions on the National Security and Intelligence Priorities and the annual threatscape report.

---

[660] Jonathan Boston, David Bagnall and Anna Barry *Foresight, insight and oversight: Enhancing long-term governance through better parliamentary scrutiny* (Institute for Governance and Policy Studies, Victoria University of Wellington, June 2019) at 11.

[661] Royal Commission report, recommendation 17.

12.41. We heard from submitters that having the Committee receive submissions on these topics would be a positive step towards informing and engaging the public on matters of national security. We support the Royal Commission's recommendations and provide further commentary on them in chapter 4 in connection with intelligence priorities and chapter 11 in connection with intelligence assessment.

12.42. In summary, then, effective parliamentary oversight is important because it enables democratic accountability, enhances the Agencies' legitimacy and promotes public confidence. In principle, a committee such as the Intelligence and Security Committee should be more actively engaged in providing robust democratic scrutiny of the Agencies and the issues their work raises. It should be as open as reasonably possible about its work. We say 'in principle' because there are some practical considerations that we will come to when we address doubts that have been raised about the practicality of this recommendation.

What would an effective Intelligence and Security Committee look like?

12.43. As noted above, oversight arrangements for intelligence and security agencies are necessarily specialised (or area specific), given that such agencies operate in secret and exercise intrusive powers. That is why New Zealand has an Inspector-General of Intelligence and Security in an oversight role rather than simply relying on the Ombudsman. There is the same need for special arrangements for parliamentary oversight of intelligence and security functions, which explains in part the establishment of parliamentary oversight bodies as statutory committees rather than as select committees under Parliament's ordinary processes.

12.44. We set out our views as to what an effective Intelligence and Security Committee would look like under four headings:

- independence
- capacity
- coverage
- transparency.

12.45. We should make it clear, however, while we recommend reconstituting the Committee along the lines of the Canadian and UK committees, we accept that it will not fully replicate those committees. Inevitably, it will have fewer resources and will have to be more modest in its ambitions.

(a) Independence

12.46. The parliamentary oversight committees in Australia, Canada and the UK are all subject, to a greater or lesser extent, to Executive power, exercised through the Prime Minister. It may be that some Executive control of such committees is inevitable, given the interests at stake and the evolving nature of parliamentary oversight of intelligence and security functions.

12.47. But one respect in which the committees in those countries differ markedly from New Zealand's is that members of the Executive (Ministers in particular, but also parliamentary Under-Secretaries) are prohibited by statute from committee membership. In New Zealand, the Prime Minister is not only a member of the Committee but generally chairs it.[662] The Minister

[662] Section 198(2) of the ISA provides that the Prime Minister may not chair a meeting of the Committee where, in the course of conducting a financial review of an agency, it is discussing any matter relating to the agency's performance and the Prime Minister is the Minister responsible for it. The section also provides for Prime Ministerial absences.

responsible for the Agencies will be on the Committee and perhaps other Ministers as well. This is inconsistent with a fundamental principle of responsible government – that Ministers, as members of the Executive, should be answerable to Parliament for activities within their portfolios. The Committee's lack of independence from the Executive, and the limited public knowledge of its activities, are unlikely to create public confidence in it as an effective oversight body.

12.48. Accordingly, we believe that no member of the Executive should be entitled to be a member of the Committee. While we will not attempt to give a detailed description of the statutory provisions necessary for an effective Committee, we envisage that the Committee's membership would remain relatively small (no more than seven or eight members) and that the ISA would continue to provide a formula for membership in terms of significant parties represented in Parliament. We also envisage that the Prime Minister would continue to make nominations, after undertaking appropriate consultation processes, which Parliament would either endorse or reject. It would also be necessary to ensure that there was some form of vetting process before the Committee's reports were made public, possibly through the Prime Minister's office.

12.49. Members of the Committee would be expected to act in a non-partisan way and in the public interest. The Chair of the Canadian committee told us that its members see themselves as acting on behalf of 38 million Canadians rather than as partisans in the political process. Likewise, members of the New Zealand Committee should see themselves as acting on behalf of all New Zealanders, rather than as representatives of particular political parties. This could be reinforced by a suitable statutory provision.[663] It would also be important that the existing distinction between the work of the Inspector-General and that of the Committee be maintained in the legislation.

(b) Capacity

12.50. There are two aspects to capacity: legal power and practical requirements.

12.51. Beginning with legal power, we consider that the ISA should be amended to make it clear that one function of the Committee is to examine the effectiveness of the Agencies. The Committee should also be empowered to consider operational matters (although it may be necessary to exclude current operations). In this context, the Committee should have the power to consider matters such as intelligence collection and production methods, particularly because these may raise important questions as to what is appropriate in a free and democratic society. This would bring the Committee's powers into line with those of the Canadian and the UK equivalents.[664] It would, however, give the New Zealand Committee a power that the Australian committee does not have. Obviously, there would have to be some coordination between the Committee and the Inspector-General to ensure there was no overlap in their work, but we do not see this as a significant problem as we see the two oversight mechanisms as operating at different levels and addressing distinct issues.

---

[663] As noted in Chapter 5, s 194(6) of the ISA provides that when performing the Committee's functions, a member of the Committee acts in their official capacity as a member of Parliament, but does not go so far as to emphasise their need for political neutrality when sitting as a Committee member.

[664] See above [12.21] – [12.28] for the functions of the Canadian and UK committees.

12.52. Turning to practical requirements, if the Committee is to undertake an expanded role, it will need more resources and will need to have independent access to classified information, including Top Secret information. Accordingly, we consider that:

- The Committee should be supported by a small secretariat of cleared staff, as is the case in Australia, Canada and the UK. We have in mind a staff of three to four cleared personnel.
- In relation to access to classified material, we understand that the convention in New Zealand, as in the UK and Australia, is that members of Parliament do not obtain security clearances to discharge relevant functions. Presumably this convention would apply to the members of a reformed Intelligence and Security Committee. It is critical that Committee members have access to the material they need to perform an effective democratic oversight function, which means they must have independent access to all forms of relevant classified material.[665] We have no view about how that should be achieved, simply that it must be done in a way that provides appropriate protection for the material. We note that even if members of Parliament are not required to obtain clearances, they will be caught by the provisions of s 78AA of the Crimes Act 1961 if they disclose classified information without authority.
- The Committee may need access to specialist technical advice from time to time. We address that further in the discussion of the Inspector-General, which follows.

(c) Coverage

12.53. In our view, the Committee's coverage needs to be expanded in two respects: the first concerns intelligence assessment; the second concerns the range of intelligence collection agencies or activities that should fall within the Committee's mandate.

12.54. The Cullen/Reddy report said that the National Assessments Bureau, as the country's principal intelligence assessment agency, should be brought within the Committee's oversight responsibilities.[666] This was not implemented in the ISA, however.

12.55. We agree that the country's primary intelligence assessment agency (or agencies) should fall within the Committee's oversight responsibilities. Intelligence assessment is intended to improve decision-making and is the finished intelligence product that Ministers and senior officials generally access; this product uses Five Eyes material and is shared with Five Eyes partners. The Royal Commission concluded that the concentration of counter-terrorism resources on the threat of Islamist extremist terrorism was inappropriate because it was not based on an informed assessment[667] and noted matters related to the coordination of assessment and effectiveness of the National Assessments Bureau in its report.[668]

---

[665] In principle, this would include sensitive material of the type referred to in s 202 of the ISA, but it may be necessary to give the Prime Minister the power to block the provision of some particularly sensitive material to the Committee in exceptional circumstances.

[666] Cullen/Reddy report recommendation 27.

[667] Royal Commission report, consolidated findings at [6].

[668] "The more general problem, as we see it, is that the two key assessment agencies were not well situated to provide assessments of emerging threats. In the case of the National Assessments Bureau, this was a result of its customer focus and its limited resources." Royal Commission Report, part 8, chapter 15 at [57]. "We were told that in 2015 the staffing level was so low as to be below a credible minimum. The 2016 Strategic Capability and Resourcing Review had envisaged growing the strategic assessments function from 21 analysts to 34 over four years. But reprioritisation over the past five years saw the increased resourcing shift to other areas. In July 2019, there were only three more analysts … than there were before the Strategic Capability and Resourcing Review."Royal Commission Report, part 8, chapter 4 at [27] – [28]. We understand that the Bureau is still yet to reach the staffing level identified in 2016.

12.56. Apart from any relevant 'customer' response, there does not appear to be any person or agency responsible for evaluating the assessment function currently performed by the National Assessments Bureau. We appreciate that the work of the National Assessments Bureau will likely be affected by government decisions in relation to the Royal Commission's recommendation that a national intelligence and security agency be established. Subject to that, we agree with the view expressed in the Cullen/Reddy report that the Committee's mandate should include oversight of the principal intelligence assessment agency.

12.57. In terms of the range of intelligence collection agencies, we have already noted that the Canadian and UK committees now have oversight functions in relation to a significantly broader range of agencies than simply the core intelligence and security agencies. For example, both have a mandate in respect of defence intelligence activities.[669] The mandate of the Australian committee is also broader than that of the New Zealand Committee, and it also has a mandate in respect of defence intelligence activities.

12.58. We recommend that consideration be given to expanding the Committee's mandate to include the power to review the effectiveness of significant intelligence collection and analysis functions in other agencies. If the Committee were to be reformed as we have recommended, its members would build up their expertise in intelligence and security issues over time. Apart from the general benefit of having more members of Parliament who were closely familiar with national security and intelligence issues, it would be useful to have that expertise brought to bear on issues arising from the work of, for example, the New Zealand Defence Force's intelligence function where they are similar to issues raised by the Agencies' work.

12.59. In addition, as we noted in chapter 3, government departments and other entities are increasing their data collection and analysis activities so as to improve their efficiency and effectiveness. This will continue to increase as private sector companies offer more products and services for obtaining, analysing and manipulating data. While much of this activity raises issues under the Privacy Act and is subject to the oversight of the Privacy Commissioner,[670] it is also relevant to the context of oversight of the Agencies. It would not be satisfactory if government departments could undertake activities without any explicit authorisation or oversight that the Agencies could not undertake without a warrant or other authorisation. A reformed Committee should be able to play a useful role in this context.

12.60. Finally on the topic of coverage, we emphasise again that the current demarcation between the roles of the Committee and of the Inspector-General should be maintained in the provisions setting out the Committee's functions.

(d) Transparency

12.61. As noted above, the Royal Commission recommended that the Committee take a more public role in the context of national security priorities, so as to promote public understanding and discussion of national security issues. If the Committee were to be reconstituted in the way we have suggested, it would have to be as open as possible about its work, so as to enhance public confidence in it and to promote the type of public understanding and discussion that the Royal Commission had in mind.

---

669 See above n 18, for the number of agencies over which the UK and Canadian Committees have oversight responsibility.

670 See, for example, Michael Webster, Privacy Commissioner "Open Source Intelligence Conference Keynote Address 2022" (2022 OSINZ Conference, Wellington, New Zealand, 22 October 2022).

12.62. As noted in chapter 4, the Committee usually meets in private but can hold public sessions. Given the experience of similar committees elsewhere, we expect that private meetings in secure facilities would continue to be the norm but that there would be some scope for greater public engagement than currently occurs. If the reformed Committee conducted an inquiry into, say, diversity in the Agencies, it could invite public submissions and hold public hearings. Even if the public were excluded from most of the Committee's meetings, greater public engagement could still be facilitated by publishing public reports. This may assist in enhancing social licence for the Agencies' work. As we have said, encouraging greater public understanding of, and engagement with, issues of national security, and with the work of the Agencies, was a major feature of the Royal Commission's report.[671]

12.63. We should emphasise, however, that the Committee will inevitably be limited in the extent to which it can discuss issues publicly.

Contrary views

12.64. Three significant doubts have emerged during our consultations:

- The first is that New Zealand Parliament is too small to accommodate our recommended changes.
- The second is that establishing the Committee on the basis we recommend is not consistent with New Zealand's practice in relation to select committees and there is no reason to subject the Agencies to a different type of parliamentary scrutiny than is given to other state agencies. It would also require greater resources.
- The third is that a reformed Committee is unnecessary.

We address each point in turn.

The New Zealand Parliament is too small

12.65. The New Zealand Parliament has 120 members (subject to small increases in some circumstances). The Cabinet is likely to involve around 28–30 members of Parliament and, with a further member as Speaker, would leave around 90 non-Executive members of Parliament eligible for membership of the Committee. By contrast:

- In Australia, the Parliamentary Joint Committee has 11 members, five from the Senate and six from the House of Representatives. A majority must be government members. Parliament is made up of 76 senators (all elected) and 151 members of the House of Representatives (all elected).
- In Canada, the committee has up to 11 members, with up to eight from the House of Commons and up to three from the Senate. Of the eight from the House of Commons, five must be members of the governing party. There are 338 members in the House of Commons (all elected), and 105 in the Senate (all appointed).
- In the UK, the Intelligence and Security Committee of Parliament has nine members drawn from the House of Lords and from the House of Commons. The House of Lords has almost 800 members (hereditary and appointed) and the House of Commons 650 members (all elected).

[671] Royal Commission report, *r*ecommendations 6 and 17.

Accordingly, in Australia, Canada and the UK, even allowing for the exclusion of members of the Executive, there are still plenty of members available to serve on the respective committees. As some of those members will have little prospect of ever being asked to join the Executive, membership of a committee such as the Intelligence and Security Committee provides an opportunity to make a meaningful contribution to the well-being of the country.

12.66. Boston, Bagnall and Barry note that New Zealand has a particularly small parliament relative to its population when compared with similarly sized democracies.[672] They go on to say:

> Consequently, MPs who are not part of the Executive branch are stretched thinly across multiple committees, especially government backbenchers, who invariably are fewer in number than MPs of opposition parties. This relatively small pool of MPs has implications for the number and size of select committees, which in turn affects the amount of business that can be conducted in the committee system.

12.67. We accept that the small size of the New Zealand Parliament creates a difficulty. Assigning seven or eight non-Executive members of Parliament to an Intelligence and Security Committee of the type that we envisage would limit their availability for other select committee work. Also problematic are the shortness of the electoral cycle (elections every three years) and the fact that some continuity of membership is necessary if the Committee is to be an effective oversight body. Boston, Bagnall and Barry say that since 1999, the average rate of turnover of members of Parliament per election has been almost 26 percent. This may make it more difficult to achieve a reasonable degree of continuity of committee membership across Parliaments.

12.68. These problems have led us to consider whether there are other options. Some consultees suggested that the membership of the current Committee could be modified to include several independent members who are not parliamentarians, but that would raise significant policy and other issues. Damian Rogers and Shaun Mawdsley have suggested that an office of Parliamentary Commissioner for Security be established, but their focus was on the restoration of the public's trust and confidence in the Agencies rather than on the performance of an oversight function.[673] Existing independent office holders, such as the Auditor-General or the Inspector-General, could assume a broader mandate in relation to the national security sector, or aspects of it, but we do not see that as filling the democratic oversight deficit. Reviews such as the present have the statutory power to examine the effectiveness of the Agencies and their contribution to national security if that is included in their terms of reference, but that type of periodic review (every five to seven years) carried out by non-parliamentarians falls short of what effective democratic oversight requires. Overall, we have been unable to identify any viable alternative to reforming the Committee along the lines we have proposed.

12.69. Ultimately, then, the decision comes down to the importance we attach as a country to having effective democratic oversight of the work of the Agencies.

---

[672] Jonathan Boston, David Bagnall and Anna Barry *Foresight, insight and oversight: Enhancing long-term governance through better parliamentary scrutiny* (Institute for Governance and Policy Studies, Victoria University of Wellington, June 2019) at 71. Sir Geoffrey Palmer KC's submission to the Standing Orders Committee in the context of the 2023 Review of Standing Orders argued that Parliament's membership should be increased from 120 to 150: see Sir Geoffrey Palmer KC "Submission to the Standing Orders Committee on the 2023 Review of Standing Orders".

[673] Damian Rogers and Shaun Mawdsley "Restoring Public Trust and Confidence in New Zealand's Intelligence and Security Agencies: Is a Parliamentary Commissioner for Security the Missing Key?" (2022) 18 *Policy Quarterly* 59.

Inconsistent with New Zealand practice

12.70. The bulk of the work of select committees in the New Zealand Parliament relates to matters of more-or-less immediate moment, such as scrutinising Bills, going through the Budget process and undertaking financial and performance reviews. Longer-term issues tend to be relegated.[674] Moreover, New Zealand does not have a dedicated cadre of backbenchers who are content to spend their parliamentary careers on the work of Parliament rather than the work of the Executive, as is the case in larger parliaments. The kind of rigorous work that we envisage for the Committee does not sit comfortably with the current approach to select committee work and would result in a more demanding committee process for the Agencies than applies to other government organisations.

12.71. We accept that but are unrepentant. It appears that currently select committees are not operating as they should. For example, in his submission to the Standing Orders Committee in connection with the 2023 Review of Standing Orders, the Clerk of the House said that, in general, select committee scrutiny is "not systematically, reliably robust. Meaningful scrutiny by select committees should be a given, and should drive better governance".[675] He highlighted particular problems in relation to the quality of performance reporting by government agencies, drawing on an Auditor-General's report.[676]

12.72. If, as the Clerk of the House suggests, the current scrutiny of departmental performance by select committees is, generally speaking, unsatisfactory and needs improvement, that is hardly a reason for rejecting change to the Committee to enable it to provide effective scrutiny of the Agencies. If a reformed Committee raises the bar, so much the better.

Resourcing

12.73. The issue of resources was raised during our consultations. Resources are, of course, always an issue, but not one that we can do anything other than acknowledge. Australia, Canada and the UK have committed significant resources to their equivalent committees in recent years. (The budget for the secretariat to the Canadian committee is around $[Can]3.5 million.) If the New Zealand Committee were to be reformed as we have suggested, it would require additional resources, albeit not on the scale of those committed to the Canadian and UK committees.

12.74. There are two points to emphasise in this context:

- First, as noted in chapter 4, the office of the Inspector-General was substantially strengthened in 2013 and received further resources to make it more effective.
- Second, the Agencies themselves have received considerable funding boosts in recent years, in 2015 and 2019 in particular.

By contrast, the Committee has stayed essentially as it was when it was set up in 1996, with only modest changes, none involving much (if anything) in the way of additional resources. It is now time to reshape it, enhance its powers and commit greater resources to it.

---

[674] Jonathan Boston, David Bagnall and Anna Barry *Foresight, insight and oversight: Enhancing long-term governance through better parliamentary scrutiny* (Institute for Governance and Policy Studies, Victoria University of Wellington, June 2019) at 227.

[675] Clerk of the House of Representatives "Parliamentary Scrutiny of the Executive: Submission on the Review of Standing Orders 2023" at 9.

[676] Above n, at 17.

An unnecessary reform?

12.75. The Agencies say that there are various mechanisms through which they are obliged to account for their effectiveness, such as the annual reports, which they must prepare under s 221 of the ISA and the Committee's annual reviews. In addition, they say that as the Inspector-General is able to consider their operational effectiveness, there is a risk of overlap or parallel inquiries as between the reformed Committee and the Inspector-General. This may suggest that they see an enhanced Committee as unnecessary.

12.76. While we agree that elements of the Agencies' effectiveness may be considered through existing mechanisms, we do not accept that the effectiveness of the Agencies in fulfilling their statutory functions is currently scrutinised in the consistent and thorough-going way necessary in a democratic society. Members of the Intelligence and Security Committee have acknowledged as much. As highlighted in chapter 4, concerns about the measurement of the effectiveness of the Agencies and the National Assessments Bureau are longstanding. The same concern was expressed in the 2014 Performance Improvement Framework of the GCSB, NZSIS and National Assessments Bureau: [677]

> At present [the New Zealand Intelligence Community] does not have processes to systematically monitor, measure and review work to make sure it is delivering its intended results. There has been a variable approach to formal reviews and informal monitoring across NZIC
>
> ...
>
> We looked to see if there was a robust set of processes in place across the NZIC that would provide clear indications to management of the results of their efforts. It does not have such processes. The closest to a feedback loop was the focus on legal compliance of processes and, while important, this does not constitute feedback as to efficiency or effectiveness of activities.

12.77. Further, as we have noted previously, in providing effective democratic oversight, an independent Intelligence and Security Committee would have to address matters in addition to the Agencies' effectiveness, for example, legislation on matters that bear on national security and intelligence, such as counter-terrorism, foreign interference and other threats, as well as policy issues about particular collection techniques or other matters of concern to the New Zealand public.

12.78. For the sake of emphasis, we say again that we do not see the issue of overlap between the work of the Committee and the Inspector-General as a problem. We envisage that the two oversight mechanisms will operate at different levels and address distinct issues and that they will coordinate their activities to ensure there is no overlap. We do not see that there will be any change to the statutory provisions intended to ensure that their work is complementary rather an overlapping.

[677] Peter Bushnell and Garry Wilson *Performance Improvement Framework: Review of the agencies in the core New Zealand Intelligence Community (NZIC)* (July 2014) at 14 and 18.

RECOMMENDATION 29

Amend the Intelligence and Security Act 2017 (ISA) to reconstitute the Intelligence and Security Committee so that:

a. members of the Executive may not be members of the Committee

b. members are selected by Parliament on the basis of nominations made by the Prime Minister and the Leader of the Opposition after consultation with each other and with the leaders of parliamentary parties both within and outside the Government. The Committee should be as representative as possible of the parties in Parliament

c. a chairperson and deputy chairperson are elected by the Committee

d. the Committee's functions are expanded to make it clear that part of its mandate is to examine the effectiveness of the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) in fulfilling their functions under the ISA, which could include examination of operational activities, such as issues relating to data collection

e. the policy, administration, expenditure and effectiveness of the National Assessments Bureau or its equivalent are brought within the Committee's mandate

f. members of the Committee are able to access all relevant classified material, including information on past operational activities

g. the Committee is supported by a small, permanent secretariat of staff holding appropriate clearances, which is independent of the Government of the day

h. the Committee has access, as required, to the panel of independent technical experts that we have recommended be established (Recommendation 32)

i. legislation that bears on national security and intelligence is referred to the Committee to allow consideration of all relevant information when Parliament is making law.

The legislation should continue to draw a distinction between the work of the Inspector-General of Intelligence and Security and that of the Committee.

Consideration should also be given to amending the Intelligence and Security Act 2017 to make it clear that members of the Committee exercise their oversight functions on behalf of all New Zealanders rather than on a party political basis.

RECOMMENDATION 30

Expand the Intelligence and Security Committee's role beyond the Government Communications Security Bureau and the New Zealand Security Intelligence Service to other agencies with significant intelligence collection and assessment functions that bear on national security, including Defence Intelligence, Customs Intelligence, Immigration Intelligence and Police Intelligence.

Inspector-General of Intelligence and Security

12.79. One of the overseas office holders we consulted described the office of the Inspector-General of Intelligence and Security in New Zealand as being 'the gold standard'. In terms of what we are considering – the legislative framework for the office – we agree with that assessment. Accordingly, there are no major changes that we would recommend.

12.80. However, a variety of relatively small points have been raised in the context of the Inspector-General. Most we address in the Routine Improvements section. Others we address here, under the headings:

- Scope of activities
- Interactions with other office holders
- Panels
- Resolution of legal disputes.

Scope of activities

12.81. We have recommended that the Intelligence and Security Committee's mandate be expanded to include the principal intelligence assessment agency (or agencies). Presumably, that will be the recommended national intelligence and security agency if the government decides to establish it. There is a question whether the Inspector-General's mandate should also be expanded to cover that agency.

12.82. In principle, we think it should. We see some value in the Intelligence and Security Committee and the Inspector-General having similar mandates in terms of coverage of agencies. More importantly, however, issues of legality and propriety could arise in the course of the assessment agency's work, whether they flow through from the work of the Agencies or derive from the work of the assessment agency itself – this also applies to complaints. This is unlikely to be an onerous role but rather one that fits in with the Inspector-General's current work.

12.83. Similarly, there is a question as to whether the Inspector-General's mandate should be extended to cover the intelligence and security activities of agencies besides the GCSB and the NZSIS, for example, the Ministry of Business, Innovation and Employment or Customs intelligence and assessment capabilities, which cooperate closely with the Agencies, or NZDI's intelligence assessment or geospatial intelligence capabilities, where intelligence is being provided to the whole of government. In part, that depends on whether the Committee's mandate is expanded; in part, it depends on what oversight mechanisms are already in place; and, in part, it depends on the value ascribed to system coherence and specialised expertise in intelligence oversight.

12.84. In relation to the first point, the Inspector-General noted in his submission to us that from 2016 onwards, there had been a move towards expanding the jurisdiction of existing oversight bodies, such as his, in Australia, Canada and the UK to cover a broad range of agencies with domestic intelligence functions, for example, in defence, police, immigration and border control. He suggested that there was much to recommend that approach in terms of seeking to encourage effective and consistent best practice across the various agencies. As will be apparent from what we have already said in this report, we are supportive of such an approach.

12.85. That said, existing oversight mechanisms are also relevant in this context. The national security and intelligence functions of NZDF and the Police fall within the mandates of their respective oversight bodies: the Inspector-General of Defence (once established) and the Independent Police Conduct Authority. Given the expertise that has been built up within the office of the Inspector-General of Intelligence and Security, it seems sensible to ensure that the expertise of that office is available to other oversight bodies when appropriate. We address this further in the next section.

Interactions with other office holders

12.86. Under s 161(1) of the ISA, the Inspector-General must have regard to function of the Auditor-General in relation to the Agencies and may consult the Auditor-General to avoid both office holders inquiring into the same matter. Under s 161(2), the Inspector-General may consult and disclose information to any of the Auditor-General, an Ombudsman, the Privacy Commissioner, a Human Rights Commissioner, the Independent Police Conduct Authority and the Public Service Commissioner. If the Inspector-General of Defence Bill is enacted, that office will be added to the list.[678]

12.87. Some of the legislation governing the listed consultees contains similar consultation powers. In particular, the Ombudsmen Act 1975 enables the Ombudsman to consult with the Inspector-General,[679] the Privacy Commissioner[680] and the Health and Disability Commissioner.[681] Similarly, under the Privacy Act 2020, the Privacy Commissioner may consult the Inspector-General, the Ombudsman and the Health and Disability Commissioner.[682] The Inspector-General of Defence will have similar powers of consultation to those of the Inspector-General if the Bill is enacted.[683]

12.88. In addition, the Ombudsmen Act contains a provision that enables the Ombudsman to transfer an inquiry to the Inspector-General, either in whole or in part, in appropriate cases.[684]

12.89. It also relevant to note that following the tragic events in the LynnMall supermarket on 3 September 2021, a joint inquiry was established, involving the Inspector-General, the Independent Police Complaints Conduct Authority and the Corrections Inspectorate. The inquiry looked into the actions of the NZSIS, the Police and the Department of Corrections in relation to the individual involved. The findings of the joint inquiry were published on 14 December 2022.[685] In his 2021–2022 annual report, the Inspector-General said that the arrangement had "worked very well and will serve as a model for future joint inquiries".[686] That type of joint inquiry does offer a mechanism for enabling the specialist skills of different oversight bodies to be utilised together during investigations.

---

678 Inspector-General of Defence Bill, sch 3.

679 Ombudsmen Act 1975, s 21C

680 Section 21A.

681 Section 21B.

682 Privacy Act 2020, s 208.

683 Inspector-General of Defence Bill, cl 26.

684 Ombudsmen Act, s 17C. For completeness, we note that under the Privacy Act, the Privacy Commissioner may investigate the actions of one of the Agencies and produce a report: Privacy Act 2020, s 95.

685 Brendan Horsley, Judge Colin Doherty and Janis Adair *Coordinated Review of the Management of the LynnMall Supermarket Attacker* (online, 14 December 2022).

686 Inspector-General of Intelligence and Security *Annual Report for the year 1 July 2021 to 30 June 2022* (November 2022) at 1 and 9.

12.90. We were interested in finding out how often the ability to consult and provide information had been exercised and whether these various office-holders met periodically to discuss issues of common concern, particularly in relation to intelligence and national security issues.

12.91. In brief, the Auditor-General indicated that there was not much crossover between the work of the Inspector-General and his office and that there had not been any consultation under s 161(2). The Privacy Commissioner said that he thought the relationship between his office that of the Inspector-General was working well, noting that his office had contributed its specialist expertise to investigations by the Inspector-General. He also noted that in 2014, his predecessor had established an oversight group of the Inspector-General, the Chief Ombudsman and the Auditor-General to coordinate and share insights about issues relating to the oversight of the Agencies. The Directors-General had occasionally joined the group to update it on developments within the Agencies. This gave rise to a suggestion to create an oversight board of the relevant oversight agencies. We understand that this grouping of the Auditor-General, the Inspector-General, the Chief Ombudsman and the Privacy Commissioner continues to meet quarterly.

12.92. Finally, the Chief Human Rights Commissioner said that he has generally been concerned about the need for coordination among the oversight bodies. During the COVID-19 crisis, he organised and convened regular informal meetings between the heads of oversight agencies to discuss the unique challenges that arose. There has been little, if any, consultation between the Inspector-General and the Human Rights Commission under s 161. He suggested it would be worth looking at the consultation and coordination approach of the multi-agency national preventative mechanism system established in New Zealand under the Crimes of Torture Act 1988 to monitor places of detention. The system was implemented to meet New Zealand's obligations under the Optional Protocol to the Convention Against Torture and other Cruel, Degrading or Inhuman Treatment or Punishment.[687]

12.93. One of the difficulties with promoting consultation among the various oversight bodies is that some may not have any cleared staff, which limits their capacity to engage in a detailed way with the Inspector-General on some aspects of his work. Despite this, we consider that there should be regular, structured consultation and discussion between the oversight agencies on matters of common concern, including in relation to intelligence and national security issues. Rather than relying on a voluntary model, we consider that there should be a statutory obligation on the oversight bodies to meet, say, at least twice a year to discuss issues of common concern and coordinate their work to the greatest extent possible. We are not sure where this statutory obligation should be located, but it may be best appearing in the enactments governing each of the oversight bodies.

12.94. We should say that the officers consulted were, in general, not in favour of creating such a statutory obligation, preferring to rely on their general authority to undertake consultation. While we understand that, we should note that one of the recurring themes of our consultations within the public sector was how much of the functioning of the national security sector depends on voluntary participation by officials in informal committees or groups. Such arrangements work well when everyone is committed to making them work and is prepared to commit resources to achieve that. But as personnel and/or organisational imperatives change, so also

[687] New Zealand has established several National Preventative Mechanisms to undertake inspections of places of detention. They are the Office of the Ombudsman, the Independent Police Conduct Authority, the Children's Commissioner and the Inspector of Service Penal Establishments. The Human Rights Commission has been appointed as the Central National Preventative Mechanism to provide coordination. See the Crimes of Torture Act 1988, ss 26–32.

can the level and quality of participation in informal groupings. This seems to us to be a context in which structural requirements have a significant role to play.

12.95. Finally, the Inspector-General has noted that, unlike the position with domestic oversight bodies, there is some doubt about his ability to discuss classified material with overseas oversight bodies. He had in mind in particular a grouping of counterparts and colleagues involved in oversight in other Five Eyes countries, known as the Five Eyes Intelligence Oversight and Review Council. The Inspector-General considers that there would be significant benefit in his being able to discuss classified issues and best practice approaches and solutions with colleagues in the Five Eyes partnership. We agree with this in principle and recommend that consideration be given to the best way of achieving this through an amendment to the ISA.

Panels

12.96. The ISA provides for the appointment of an advisory panel of two people to advise the Inspector-General and, if necessary, to report to the Prime Minister. The Inspector-General would like the number of members to be increased to three to meet difficulties that have arisen when one or other member has been unavailable or there has been a vacancy in the panel. Given the Inspector-General's experience, this seems to us to be a reasonable request.

12.97. More significantly, the Inspector-General would like access to a technical advisory panel, similar to that available to the UK Investigatory Powers Commissioner's Office. This would be a panel of, say, three independent technical experts. Our experience in conducting this review has persuaded us that it is important for lay people (even knowledgeable lay people) to have access to experienced and independent technical personnel. We think it undesirable that the Inspector-General should have to rely exclusively on the Agencies for technical assistance or on such technical knowledge as his staff happen to have. The same applies to the Intelligence and Security Committee and the Commissioners of Intelligence Warrants – both would benefit from being able to consult with one or more independent technical experts from time to time.

12.98. We therefore recommend that the ISA be amended to provide for the appointment of a three-person panel of independent technical experts. These experts could be called on, either individually or collectively, by any of the Intelligence and Security Committee, the Inspector-General and the Commissioners, as required. We make no comment about the appointment process for the panel, other than to say that the Chair of the Intelligence and Security Committee, the Inspector-General and the Chief Commissioner of Intelligence Warrants should be consulted before any appointments are made to ensure that experts with the right type of technical skills are appointed.

Resolution of legal disputes

12.99. As we noted in chapter 4, there is likely to be little judicial interpretation of the provisions of the ISA as legal disputes about its interpretation are unlikely to come before the courts. Rather, if the Inspector-General has a view about the proper interpretation of the ISA that an Agency disagrees with, the Agency may seek an opinion from the Solicitor-General. That opinion will be directive as far as the Agency is concerned but will not be binding on the Inspector-General given that he is an independent statutory officer. While this is likely to arise infrequently, we consider it undesirable that differences of opinion between the Solicitor-General and the Inspector-General are effectively left with no clear route available for their resolution.

12.100. We wondered whether the ISA should be amended to insert a provision similar to one in the Inquiries Act 2013, which provides that questions of law can be referred to the High Court for determination.[688] The Inspector-General was not attracted by this suggestion and doubted that this was necessary, nor was he enthusiastic about our further suggestion that the Commissioners could provide definitive rulings, given that they were party to the issue of warrants. He considered that the Declaratory Judgments Act 1908 provided a satisfactory mechanism to take disputed questions of law to the High Court. We have some doubts about the efficacy of that mechanism, but we will not take the issue further here.

RECOMMENDATION 31

Amend the Intelligence and Security Act 2017 (ISA) to provide for the Inspector-General of Intelligence and Security to:

a. have regular, structured consultation and discussion with other oversight agencies on matters of common concern, including those on intelligence and national security

b. be able to discuss classified material with overseas oversight bodies in a manner consistent with its classification

c. be supported by a three-person advisory panel, which is an expansion from the current two-person panel provided for by section 169 (Membership of advisory panel) of the ISA

d. have an expanded mandate to include the principal intelligence assessment agency (or agencies) in alignment with any corresponding changes to the Intelligence and Security Committee.

RECOMMENDATION 32

Amend the Intelligence and Security Act 2017 to provide for the appointment of a three-person panel of independent technical experts that is available to support the Inspector-General of Intelligence and Security, the Intelligence and Security Committee and Commissioners of Intelligence Warrants to perform their functions and the Inspector-General, the Committee and Chief Commissioner should be consulted before any appointments are made to the panel.

Commissioners of intelligence warrants

12.101. Ignoring for these purposes the changes we have recommended to the warranting provisions, there are only three matters in respect of which we recommend changes to the ISA in relation to Commissioners of Intelligence Warrants. They are:

- First, we consider that the ISA should be amended to allow the Commissioners to have access, as required, to the panel of independent technical experts that we have recommended be established. We think it undesirable that the only source of technical information available to the Commissioners is from the Agencies.

[688] Inquiries Act 2013, s 34.

- Second, we consider that provision should be made in the ISA for the Commissioners, through the Chief Commissioner, to issue Advisory Notices similar to one issued by the Investigatory Powers Commissioner's Office (IPCO) in the UK.[689] The purpose of the ICPO's Advisory Notice 1/2018 was described as:

  > … to provide advice and information to public authorities and to the general public as to the general approach that Judicial Commissioners will adopt under the [Investigatory Powers Act 2016] when deciding whether to approve decisions to issue warrants, authorisations and notices. It is also intended to provide assistance and guidance to the Judicial Commissioners, with a view to achieving consistency of approach, although it is not binding on them.

  While circumstances in the UK are different, in the sense that the IPCO deals with many more agencies than the two the New Zealand Commissioners deal with, and there are more Judicial Commissioners than the three in New Zealand, a document such as the Advisory Notice 1/2018 would serve a useful function. It would provide a concise statement of approach that would be helpful to the Agencies, to the Minister and to the Inspector-General, as well as to the Commissioners themselves.[690] Most importantly, it would give members of the public some insight into how the Commissioners exercise their responsibilities, shedding some light on what is otherwise an opaque process.

- Third, we consider that a provision should be inserted into the ISA to enable discussion between the Inspector-General and Commissioners about issues of common interest in way that does not affect the independence that the Inspector-General and the Commissioners must have when performing their functions. It should provide that the Inspector-General and the Commissioners should meet at least once a year.

12.102. The reason for this third recommendation is that the Inspector-General reviews every warrant after it has been issued. If his review identifies an irregularity, the Inspector-General may report the irregularity to the Minister and (in the case of Type 1 warrants) to the Chief Commissioner. The irregularity does not affect the validity of the warrant, however, or anything done under it.[691] It may be useful for the Inspector-General and the Commissioners to meet to discuss irregularities, especially if they raise broader issues about the way an Agency is approaching warrant applications. Given the need to maintain the independence of all concerned, the focus of the discussion would be on lessons for the future, not recriminations about the past.

12.103. In addition, the Inspector-General may well identify general issues during his reviews that he could usefully discuss with the Commissioners. We note that the Inspector-General has produced two reports on warrants. Reading those would not undermine the independence of the Commissioners. Similarly, a general discussion arising out of the Inspector-General's experience with reviews could be conducted without compromising either the appearance or fact of independence on both sides.

12.104. Apart from that, there may be issues such as new technological developments that the Inspector-General could usefully discuss with the Commissioners, perhaps in the context of a combined technical briefing. We were told that discussions and seminars of this type occur

[689] Issued under s 232(2) of the Investigatory Powers Act 2016 (UK).

[690] We recognise that the role of the Judicial Commissioners in the UK is not identical to that of the New Zealand Commissioner of Intelligence Warrants, but such a document would be useful as an expression of the judicial officer's view on the exercise of their responsibilities.

[691] Intelligence and Security Act 2017, s 163(2).

within the UK Investigatory Powers Commissioner's Office between, on the one hand, the Commissioners who issue warrants and, on the other, the group who reviews them. We were told that this occurred in a way that did not compromise the independence of either Commissioners or the reviewers.

12.105. Finally, the Department of the Prime Minister and Cabinet raised an issue about the ISA's requirement that Commissioners be retired High Court judges. It was said that the pool of retired High Court judges is small and therefore not as diverse or resilient as might be desirable. This can lead to difficulties in times of emergency, for example, during COVID-19. The question was raised whether New Zealand could follow the Canadian model and have a group of serving judges perform the Commissioners' roles as part of their ordinary judicial work.

12.106. Typically (although not uniformly) in comparable countries, intelligence and national security warrants are issued by judges or former judges, although the Executive, through a relevant Minister, generally has some role in the process. This is consistent with international best practice, and both the UN Special Rapporteur on the right to privacy and the UN Human Rights Committee have noted with concern the absence in New Zealand of judicial involvement in authorisation of interception warrants for non-New Zealanders.[692] Judicial experience, skills and objectivity make judges, whether sitting or retired, particularly well-suited to the role. Importantly, the public are likely to take some comfort from the fact that a person with a judicial background is required to consider whether the necessary tests are met for the issue of a warrant.

12.107. But we do not have a strong view as to whether this work should be undertaken by retired or sitting High Court judges. Sitting judges do, of course, issue interception warrants in other contexts. We accept that it may well be easier to accommodate emergency situations such as pandemics if sitting judges are involved. A further advantage that having sitting judges would bring is that, if there were issues about the meaning of relevant provisions of the ISA, it would be easier to obtain binding rulings, which would fill what we think is presently a significant gap in the ISA. In this context, we note that when the Cullen/Reddy report recommended the expansion of the pool of Commissioners from one to three, it raised the possibility of some Commissioners being sitting, rather than retired, judges. The report identified the benefit of having sitting judges as that "they could also be designated to hear cases involving security sensitive information, allowing their knowledge and expertise to be taken advantage of more widely".[693]

12.108. If the work were to be undertaken by sitting judges, it would be necessary to have a small pool of, say, four High Court judges who could deal with warrant applications.[694] There would have to be a reworking of the provisions dealing with the respective roles of the Minister and the judges as it would not be appropriate to have the type of collaborative process between Ministers and serving judges that the ISA currently contemplates. Rather, the Minister would have an initial filtering role and would have to approve an application being made to the court. Moreover, consideration would have to be given to how Commissioners perform the other roles that they have under the ISA.

---

[692] *Report of the Special Rapporteur on the right to privacy* UN Doc A/HRC/34/60 (6 September 2017) at [14]; *Concluding observations on the sixth periodic report of New Zealand* CCPR/C/NZL/CO/6 (28 April 2016) at [15].

[693] *Cullen/Reddy report* at [6.90].

[694] This could include retired judges who hold warrants as acting High Court judges.

12.109. We have had a preliminary discussion with the Chief Justice about the possibility of sitting High Court judges undertaking the role of issuing warrants. She agreed, in principle, that it should be possible to develop a workable model. However, it would require considerable further policy work.

RECOMMENDATION 33

Amend the Intelligence and Security Act 2017 to provide that the Commissioners of Intelligence Warrants:

a. have access, as required, to the panel of independent technical experts that we have recommended be established (Recommendation 32)

b. through the Chief Commissioner, have the power to issue advisory notices similar to one issued the Investigatory Powers Commissioner's Office in the United Kingdom

c. are required to have periodic discussion, at least once a year, with the Inspector-General of Intelligence and Security (the Inspector-General) about issues of common interest, in a way that does not affect the independence that the Inspector-General and the Commissioners must bring to bear when performing their functions

Conclusion

12.110. The major change recommended in relation to the three oversight mechanisms discussed in this chapter concerns the Intelligence and Security Committee. Without a restructured Committee with greater independence from the Executive, an increased mandate, enhanced powers and greater resources, New Zealand will lack effective democratic oversight of the Agencies and the intelligence community more broadly. In our view, it is now time to rectify that deficiency in our oversight arrangements and go some way to catching up with what comparable countries are doing.

SECTION

06

Summary of recommendations

SUMMARY OF RECOMMENDATIONS

Below is a summary of the recommendations by chapter as they appear in our report.

Chapter 3 – Aotearoa New Zealand's national security and intelligence community: An overview

Recommendation 1

To assist in the effective implementation of the Intelligence and Security Act 2017 (ISA), a coherent and consistent approach should be adopted in legislation governing the wider intelligence and security community. Consideration should be given to addressing legislative gaps and inconsistencies across the legislation governing the wider intelligence and security community, especially where the legislation hinders effective cooperation among New Zealand's intelligence community and the legislative frameworks applying to similar activities undertaken by different agencies differ. In particular, there should be appropriate statutory recognition for the intelligence and security functions within the New Zealand Defence Force and the New Zealand Police, especially in light of section 13 of the ISA.

Chapter 5 – Protection of national security: Reflecting New Zealand's identity

Recommendation 2

Amend section 4 (Interpretation) of the Intelligence and Security Act 2017 to include a definition of "protection of national security" along the following lines:

> **"protection of national security"** means the protection of New Zealand, its communities and people from activities that are threats because they undermine, or seek to undermine, one or more of New Zealand's—
>
> (a) territorial integrity and safety, including the safety of its communities and people;
>
> (b) sovereignty, democratic institutions, processes and values;
>
> (c) multi-cultural and diverse social fabric; and
>
> (d) essential interests, including its critical infrastructure and governmental operations;
>
> and includes identifying and enabling the assessment of such threats.

with the possible addition of wording such as:

> Such activities include, but are not limited to, terrorism, espionage, sabotage, violent extremism, insurrection, foreign interference, cyber threats and serious transnational crime.

Recommendation 3

Make publicly available a full description of the process by which the Government's priorities for the collection and analysis of intelligence by the Government Communications Security Bureau and the New Zealand Security Intelligence Service (the Agencies) under section 10 of the Intelligence and Security Act 2017 are developed.

Require the publication of the Agencies' intelligence and security priorities, with as much specificity as legitimate national security considerations permit.

Recommendation 4

Amend section 3(c) (Purpose) of the Intelligence and Security Act 2017 to give effect to te Tiriti o Waitangi/the Treaty of Waitangi and the multi-cultural and diverse nature of New Zealand society, along the following lines (with corresponding amendments to section 17 (General duties)):

> The purpose of this Act is to protect New Zealand as a free, open, and democratic society by—
>
> (c) ensuring that the functions of the intelligence and security agencies are performed—
>
> (i) in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; and
>
> **(ii) in accordance with the Crown's responsibilities to Māori under te Tiriti o Waitangi/the Treaty of Waitangi;**
>
> **(iii) in a manner that reflects New Zealand's multi-cultural and diverse society;**
>
> **(iv) in the performance of its operational functions, independently and impartially;**
>
> (iv) with integrity and professionalism; and
>
> (v) in a manner that facilitates effective democratic oversight;

Recommendation 5

Retain section 19 (Activities of the intelligence and security agency not to limit freedom of expression) of the Intelligence and Security Act 2017 without amendment.

Chapter 6 – How intelligence and security agencies gather information

Recommendation 6

Retain the lawfulness/unlawfulness criteria that govern the warranting framework in sections 48 and 49 (Authorisations) of the Intelligence and Security Act 2017, subject to the following qualifications.

a. If the lawfulness of a proposed activity by an intelligence and security agency in performing its functions, duties or powers is uncertain, a warrant to carry out the activity should be sought.

b. A warrant should be sought where the Agencies wish to obtain access to hacked and leaked datasets and sensitive datasets developed by third parties from publicly available material, such as facial images.

c. Where the Agencies seek to develop sensitive datasets themselves from publicly available material, they should be required to obtain a warrant or other form of authorisation to do so.

Chapter 7 – The warranting framework

Recommendation 7
Removal of Type 1 / Type 2 warrant distinction

Remove the distinction between Type 1 warrants (Intelligence warrant in respect of New Zealanders) and Type 2 warrants (Intelligence warrant in respect of non-New Zealanders) in the Intelligence and Security Act 2017 (ISA).

a. Warrants for the protection of national security in respect of non-New Zealanders should be assessed according to the same criteria as apply to warrants for the protection of national security in respect of New Zealanders.

b. Warrants authorising activities to contribute to New Zealand's international relations and well-being or economic well-being, in respect of New Zealanders, should continue to be assessed against the current criteria in section 59 and the criteria in section 61 of the ISA; warrants authorising activities to contribute to New Zealand's international relations and well-being or economic well-being in respect of non-New Zealanders should continue to be assessed against the criteria in sections 60 and 61 of the ISA.

c. All intelligence warrants should be jointly approved by the authorising Minister and a Commissioner of Intelligence Warrants, who can impose restrictions and conditions on the authorisations.

Recommendation 8
Applications for warrants

Update section 55 (Application for issue of intelligence warrant) of the Intelligence and Security Act 2017 (ISA) so that the Government Communications Security Bureau and the New Zealand Security Intelligence Service (the Agencies) are required to provide greater clarity and detail when seeking a warrant, and require the following information to be included as part of the warrant application:

a. the purpose of the intelligence warrant applied for

b. the functions to which the warrant relates

c. the operational objective of the warrant and details of the activity proposed to be carried out under the warrant

d. the grounds on which the application is made

e. the arguments for and against the grant of the warrant, including any legal issues that arise in connection with the proposed warrant

f. the information relied upon to meet the requirements of section 61 of the ISA (dealing with necessity and proportionality – such as the likelihood of third-party information being collected and the approach that will be taken to data retention, use and disposal)

g. a statement in which the Director-General making the application confirms that all information relevant to the decision whether to issue a warrant that is known to the Agency has been set out in the application and is true and correct

h. if the application is for a renewal or a repeat warrant, the application should specifically address why the authorisation should be continued, and the value of the information obtained under the previous warrants.

Recommendation 9
Duty of candour

Amend section 17 (General duties) of the Intelligence and Security Act 2017 to include an express reference to the duty of candour with which the Government Communications Security Bureau or the New Zealand Security Intelligence Service must act when performing relevant functions.

Recommendation 10
Warrants targeting a class

Retain in section 67 (Authorised activities) of the Intelligence and Security Act 2017 (ISA) the ability to obtain an intelligence warrant for a class of persons, subject to:

a. the provision of additional information as part of the warrant application:

   i. A class of persons is defined with as much specificity as possible for the authorisation

   ii. Information is provided on the particular characteristics that the persons in the class share or the common activities in which they are involved

   iii. The process for confirming an individual falls within the scope of the class is set out in the application, including the criteria to be used and that this is necessary and proportionate

b. further policy work being undertaken with a view to potentially amending the ISA to more clearly identify when it is appropriate to determine that an individual fits within an existing class warrant or where it is appropriate to make a new, specific, warrant application in respect of that individual.

Recommendation 11
Necessity and proportionality

Give greater statutory direction as to how the necessity and proportionality requirements are to be applied:

a. Amend section 61 (Additional criteria for issue of intelligence warrant) of the Intelligence and Security Act 2017 to include that:

   i. the proposed activities authorised under the warrant must be necessary both for the section 9 purpose of the warrant and to fulfil a function of the Government Communications Security Bureau or the New Zealand Security Intelligence Service

   ii. the proposed activity must be proportionate to the operational objective for which it is to be carried out

   iii. the operational objective of the warrant cannot reasonably be achieved by a less intrusive means

   iv. the proposed activity is rationally connected to the operational objective of the warrant

v. satisfactory arrangements are in place to ensure that individuals' reasonable expectations of privacy in personal information are taken into account.

b. Give statutory recognition to the requirement that an assessment of necessity and proportionality must apply at appropriate stages during the process of undertaking activities authorised under a warrant, not simply at the point at which a warrant is issued.

Recommendation 12
Reporting on the purpose of warrants

Amend the Intelligence and Security Act 2017 to enhance transparency over the purpose for which warrants are issued and the extent of the acquisition of bulk datasets for target discovery purposes as follows.

a. Amend section 206 (Issue of ministerial policy statements) to include the requirement for a ministerial policy statement on the acquisition of bulk datasets.

b. Amend section 83 (Register of intelligence warrants) to include in the register of intelligence warrants information on the primary purpose under section 9 for which the warrant was issued (for example national security or international relations and well-being); the function under sections 10, 11 or 12 to which the warrant relates; and where the purpose is the acquisition of bulk datasets.

c. Amend section 221(2)(c) (Annual reports of intelligence and security agencies) to include in the annual report information on the number of applications according to the primary purpose for which a warrant was sought, and where bulk datasets are acquired.

Chapter 8 – Retention and disposal of information

Recommendation 13

Amend sections 102 to 104 (Destruction and retention of information) of the Intelligence and Security Act 2017 (ISA) to make them fit for purpose.

a. Amend section 102(2) (Destruction of unauthorised information) to replace the reference to "unauthorised information must be destroyed immediately" with "unauthorised information must be destroyed as soon as practicable".

b. Amend section 102(2)(a) to include the issuance of urgent intelligence warrants and very urgent authorisations, in addition to "intelligence warrants", as exceptions to the requirement to destroy unauthorised information.

c. Clarify the interpretation of what is and what is not "outside the scope of an authorisation" in section 102 of the ISA.

d. Amend section 103 (Destruction of irrelevant information) to remove the reference to "irrelevant information" and replace with a requirement to destroy information collected within the scope of an authorised activity unless its retention is necessary for a purpose for which a warrant may be granted and to fulfil the functions of the Government Communications Security Bureau and the New Zealand Security Intelligence Service.

e. Amend section 103(3) to add a proviso that the destruction of information is subject to retention where it is required to enable the exercise of the functions of an oversight body, or if it has been destroyed, then a record of this is kept.

f. Amend section 104(2) (Retention of incidentally obtained information) to explicitly name the agencies in New Zealand, in addition to the New Zealand Police and New Zealand Defence Force, with enforcement powers, including the New Zealand Customs Service and Ministry for Primary Industries, with which the Agencies may share incidentally obtained information, while still retaining the ability for the Director-General to determine whether any other public authority should receive the information.

Recommendation 14

Provide additional resources to the Government Communications Security Bureau and the New Zealand Security Intelligence Service to enable them to declassify information for preservation with Archives NZ, given the importance of public records for Government accountability.

Recommendation 15

Adopt a coherent framework across the Intelligence and Security Act 2017, a ministerial policy statement and the policies of the Government Communications Security Bureau and the New Zealand Security Intelligence Service's (the Agencies) for the retention and disposal of all information obtained, collected, created and/or managed by the Agencies in the course of exercising their statutory functions, including information that is obtained under an authorisation, as well as by other lawful means. This should include the following elements.

a. Information management policies should apply throughout the intelligence cycle.

b. The necessity and proportionality tests should apply throughout the process of examination, use, retention and disposal of information.

c. Access and analysis of personal information should be limited to designated persons and subject to record keeping and audit requirements.

d. The rules around retention periods for all classes of information should be specified.

e. The manner of destruction or disposal should be specified.

f. The applicable principles, policies and procedures for information retention and disposal should be made public to the greatest extent possible.

Chapter 9 – Obtaining information from public and private-sector organisations

Recommendation 16

With respect to the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) (the Agencies) having direct access to database information held by other public sector agencies

a. Amend Schedule 2 (Databases accessible to the Agencies) of the Intelligence and Security Act 2017 to remove the list of databases accessible to the Agencies, but retain the names of the holder agencies (eg, New Zealand Police, New Zealand Customs Service) with which either the GCSB or the NZSIS may enter into direct access agreements.

b. The Government should consider undertaking further policy work on the appropriateness of the Agencies having direct access to non-public sector agency databases containing information in respect of which there may be a reasonable expectation of privacy, and if so, whether such access

should come under the umbrella of a broader direct access agreements regime or another form of authorisation. Any such access should be subject to specified and written agreements with the database holder, which would be reviewed by the Privacy Commissioner and Inspector-General and subject to transparency and reporting requirements.

c. The Government should consider requiring the Minister responsible for the Agency and the Minister responsible for the holding agency to submit a joint report to the Intelligence and Security Committee within 12 months of the review of a direct access agreement commencing.

Recommendation 17

The Government should undertake policy work to determine whether the business records directions regime, which enables the Government Communications Security Bureau and the New Zealand Security Intelligence Service to obtain business records from telecommunications network operators and financial service providers, should be extended to other business agencies, and this should include consultation with the potentially affected businesses and the wider public.

Recommendation 18

With respect to accessing restricted information that is specified in the Intelligence and Security Act 2017 (ISA) as information to which access is restricted by another statute:

a. The Department of the Prime Minister and Cabinet should work with the Government Communications Security Bureau and the New Zealand Security Intelligence Service (the Agencies), and other Government agencies, to determine whether any further information should be brought within the restricted information regime of the ISA.

b. The Government should consider amending the ISA to enable other domestic agencies to proactively share information they are otherwise prevented by statute from sharing with the Agencies if they believe on reasonable grounds the disclosure of that information is necessary or desirable for the maintenance of New Zealand's national security and the disclosure is subject to appropriate controls.

Chapter 10 – Inter-agency cooperation and information sharing

Recommendation 19

The Government should consider amending section 13 (Cooperation with other public authorities to facilitate their functions) of the Intelligence and Security Act 2017 to clarify the scope of "cooperation" under section 13(1)(a) and the provision of "advice and assistance" under section 13(1)(b) and how this distinction operates in the context of joint operations.

Recommendation 20

The Government Communications Security Bureau and the New Zealand Security Intelligence Service (the Agencies) and other domestic agencies with which the Agencies cooperate in order to respond to an imminent threat to life or safety under section 14 of the Intelligence and Security Act 2017 (ISA), should consider how any new or existing joint operating protocols capture the concept of an "imminent" threat to life or safety and the range of potential threat activity that may fall under section 14 and how they can be improved to support efficient and effective cooperation should such situations arise.

Recommendation 21

Amend the Customs and Excise Act 2018 to enable the New Zealand Customs Service to collect and share information pertaining to the functions of the Government Communications Security Bureau or the New Zealand Security Intelligence Service to facilitate cooperation under the Intelligence and Security Act 2017.

Recommendation 22

The Government should drive an approach to information sharing among domestic agencies that appropriately balances the need to share with the need to know to facilitate the protection of New Zealand's national security. This should include implementing the Information Security Classification Policy 2022 in a way that ensures the appropriate classification of information and encourages the declassification of information so that it can be used to respond to national security concerns.

Recommendation 23

With respect to the recently revised and reissued ministerial policy statement (MPS) on cooperation with overseas public authorities, which sets out the general requirements for the on-sharing of New Zealand intelligence:

a. To improve transparency relating to information sharing with overseas public authorities, the public should be provided with information about:
    i. the criteria used to grant 'approved party' status for sharing intelligence with foreign partners
    ii. the time period for which a standing ministerial authorisation for sharing intelligence is approved
    iii. whether the time period is adequate if circumstances change
    iv. what factors would trigger a review of the status of the overseas public authority with which intelligence is shared.
b. The MPS on cooperation should be re-evaluated during its next periodic review in light of further experience with implementing the MPS and the related joint policy statement on managing human rights risks in overseas cooperation.

Chapter 11 – Assessing and using intelligence

Recommendation 24

Amend the Intelligence and Security Act 2017 (ISA) to require the Director of the National Assessments Bureau to regularly consult the Leader of the Opposition, in line with the obligations placed on the Directors-General of the Government Communications Security Bureau and New Zealand Security Intelligence Service under section 20 of the ISA.

Recommendation 25

The National Assessments Bureau should produce a classified independent annual threatscape report to inform the intelligence priority-setting process by Ministers. The Bureau should also publish an unclassified version of the annual threatscape report, including to support a public hearing and submissions to the Intelligence and Security Committee on New Zealand's changing threatscape.

Recommendation 26

Amend the Intelligence and Security Act 2017 to explicitly include the ability for the New Zealand Security Intelligence Service to issue warnings to mitigate threats to national security and make an appropriate amendment to section 16 (Functions of intelligence and security agencies do not include enforcement).

Recommendation 27

The Government should undertake further policy work as a priority to determine whether the Intelligence and Security Act 2017 should be amended to include ability for the Government Communications Security Bureau and/or the New Zealand Security Intelligence Service to undertake threat disruption activities (beyond giving warnings), including cyber threat disruption activities. This would need to consider the scope of any such regime, whether it should include otherwise unlawful threat mitigation activities, the appropriate authorisation regime, limits, safeguards and oversight mechanisms.

Recommendation 28

Amend section 220 (Use of information provided for security assessment clearance) of the Intelligence and Security Act 2017 to include an exception to enable the disclosure of vetting information where the Director-General considers that there are reasonable grounds to believe there is a serious threat to the health or safety of any person and the proposed disclosure would prevent or lessen that threat; and require reporting to the responsible Minister and the Inspector-General of Intelligence and Security in the event of any such disclosure.

Chapter 12 – Oversight: Recommended changes

Recommendation 29

Amend the Intelligence and Security Act 2017 (ISA) to reconstitute the Intelligence and Security Committee so that:

a. members of the Executive may not be members of the Committee

b. members are selected by Parliament on the basis of nominations made by the Prime Minister and the Leader of the Opposition after consultation with each other and with the leaders of parliamentary parties both within and outside the Government. The Committee should be as representative as possible of the parties in Parliament

c. a chairperson and deputy chairperson are elected by the Committee

d. the Committee's functions are expanded to make it clear that part of its mandate is to examine the effectiveness of the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) in fulfilling their functions under the ISA, which could include examination of operational activities, such as issues relating to data collection

e. the policy, administration, expenditure and effectiveness of the National Assessments Bureau or its equivalent are brought within the Committee's mandate

f. members of the Committee are able to access all relevant classified material, including information on past operational activities

g. the Committee is supported by a small, permanent secretariat of staff holding appropriate clearances, which is independent of the Government of the day

h. the Committee has access, as required, to the panel of independent technical experts that we have recommended be established (Recommendation 32)

i. legislation that bears on national security and intelligence is referred to the Committee to allow consideration of all relevant information when Parliament is making law.

The legislation should continue to draw a distinction between the work of the Inspector-General of Intelligence and Security and that of the Committee.

Consideration should also be given to amending the Intelligence and Security Act 2017 to make it clear that members of the Committee exercise their oversight functions on behalf of all New Zealanders rather than on a party political basis.

Recommendation 30

Expand the Intelligence and Security Committee's role beyond the Government Communications Security Bureau and the New Zealand Security Intelligence Service to other agencies with significant intelligence collection and assessment functions that bear on national security, including Defence Intelligence, Customs Intelligence, Immigration Intelligence and Police Intelligence.

Recommendation 31

Amend the Intelligence and Security Act 2017 (ISA) to provide for the Inspector-General of Intelligence and Security to:

a. have regular, structured consultation and discussion with other oversight agencies on matters of common concern, including those on intelligence and national security

b. be able to discuss classified material with overseas oversight bodies in a manner consistent with its classification

c. be supported by a three-person advisory panel, which is an expansion from the current two-person panel provided for by section 169 (Membership of advisory panel) of the ISA

d. have an expanded mandate to include the principal intelligence assessment agency (or agencies) in alignment with any corresponding changes to the Intelligence and Security Committee.

Recommendation 32

Amend the Intelligence and Security Act 2017 to provide for the appointment of a three-person panel of independent technical experts that is available to support the Inspector-General of Intelligence and Security, the Intelligence and Security Committee and Commissioners of Intelligence Warrants to perform their functions and the Inspector-General, the Committee and Chief Commissioner should be consulted before any appointments are made to the panel.

Recommendation 33

Amend the Intelligence and Security Act 2017 to provide that the Commissioners of Intelligence Warrants:

a. have access, as required, to the panel of independent technical experts that we have recommended be established (Recommendation 32)

b. through the Chief Commissioner, have the power to issue advisory notices similar to one issued the Investigatory Powers Commissioner's Office in the United Kingdom

c. are required to have periodic discussion, at least once a year, with the Inspector-General of Intelligence and Security (the Inspector-General) about issues of common interest, in a way that does not affect the independence that the Inspector-General and the Commissioners must bring to bear when performing their functions

APPENDICES

Appendix A
Terms of reference

2022 Review of the Intelligence and Security Act

Under section 236(1) of the Intelligence and Security Act 2017 ("the Act"), the Prime Minister, the Right Honourable Jacinda Ardern, has appointed the Honourable Sir Terence Arnold KNZM, and Matanuku Mahuika, to carry out a review of the intelligence and security agencies and the Act. The Prime Minister has also appointed Dr Penelope Ridings MNZM to act as a special advisor to the review.

Under section 236(3)(a) of the Act, the Prime Minister has specified the following terms of reference for the review.

Terms of Reference

Section 235 of the Act requires periodic reviews of the Act and the intelligence and security agencies. The review has been brought forward to commence as soon as practicable from July 2021 to respond to the issues raised in the Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain ("RCOI report") that relate to the Act.

The first periodic review of the relevant legislation and intelligence agencies was conducted by Sir Michael Cullen and Dame Patsy Reddy in 2016 ("Cullen-Reddy review"). The Cullen-Reddy review was a fundamental review that resulted in substantial changes to the legislative framework. The 2022 review is not intended to replicate the scope of the 2016 review, or be a first principles review of the Act. The intent of this review is to understand what improvements need to be made, if any, so that the Act is clear, effective, and fit for purpose, as well as considering the relevant matters raised by the RCOI report.

1. The purpose of this periodic statutory review is to:

1.1. determine whether improvements could be made to the Act to ensure it continues to be effective, clear and fit for purpose; and

1.2. consider the recommendations and issues related to the Act that were raised in the Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain (RCOI).

2. The review will have particular regard to the following matters:

2.1. whether the Act appropriately balances national, community and individual security with individual privacy and other rights;

2.2. whether the Act sufficiently enables and controls target discovery activity by the intelligence and security agencies;

2.3. whether the authorisation framework under the Act can be improved to better serve the purpose of the Act;

2.4. whether the Act adequately provides, and has appropriate protections and oversight in place, for the collection of intelligence by both intelligence and security agencies. In particular the processing, analysis, retention and destruction of collected information/data;

2.5. how the Act may best enable the intelligence and security agencies to appropriately and effectively cooperate and share information with New Zealand government agencies and other partners;

2.6. any other matters that arise during the course of the review, as agreed by the Prime Minister and notified in writing in the *New Zealand Gazette*.

3. When determining how to conduct the review, the reviewers will take into account:

3.1. the principles agreed by Cabinet to guide the RCOI response;

3.2. that the review should be underpinned by Te Tiriti o Waitangi and its principles;

3.3. that the review should enhance trust and confidence in the intelligence and security agencies;

3.4. the need for the law to provide clear and understandable parameters of operation;

3.5. that the establishment of a new national and intelligence security agency (recommendation 2 of the RCOI) is being considered by the Department of Prime Minister and Cabinet (DPMC) as part of a review of the overarching national security policy settings and the reviewers will need to be cognisant of that work as it develops;

3.6. that the structure and current separation of the intelligence and security agencies will be considered as part of the DPMC's work on the overarching national security policy settings.

4. How the review is conducted

4.1. The review will need to meet communities' expectations of transparency as far as possible, and a wide range of members of the public should have the opportunity to express their views on issues relating to the review.

4.2. A special advisor has been made available to the reviewers to assist with the review.

4.3. The Prime Minister has specified, under section 236(3)(c) of the Act, that the review is to be concluded by 31 January 2023.

Dated at Wellington this 2nd day of March 2022.
RT HON JACINDA ARDERN, Prime Minister.

Appendix B
Authorisation framework

Intelligence and Security Act 2017 – Part 4

Principles we used to guide the authorisation framework recommendations

- **Purpose of intelligence**: The purpose of intelligence is to protect New Zealand as a free, open and democratic society, underpinned by the rule of law.
- **Human rights**: Human rights should be recognised and respected.
- **Transparency**: Social licence requires that there be as much transparency as possible in the way that the Government Communications Security Bureau and the New Zealand Security Intelligence Service ('the Agencies') operate.
- **Certainty and practicality**: The warranting framework should be certain and able to be implemented effectively.
- **Technology neutral**: The warranting framework needs to be technology neutral even as available technologies change and evolve.

Summary of recommendations for improvement

Below is a summary of the recommendations relating to the authorisation framework, including the retention and disposal of information obtained under a warrant.

Structure of the authorisation framework

- A threats-based definition of the protection of national security is provided.[695]
- The Type 1/Type 2 distinction is removed.
- All authorisations go through the same application and approval process.
- Warrants against New Zealanders and non-New Zealanders for the protection of national security are assessed by reference to the same criteria.
- Warrants authorising activities to contribute to New Zealand's international relations and well-being or economic well-being in respect of *New Zealanders* will continue to be assessed against the current criteria in s 59 and the criteria in s 61 of the Intelligence and Security Act 2017 (ISA).

[695] As suggested in chapter 5: "**protection of national security"** means the protection of New Zealand, its communities and people from activities that are threats because they undermine, or seek to undermine, one or more of New Zealand's territorial integrity and safety, including the safety of its communities and people; sovereignty, democratic institutions, processes and values; multi-cultural and diverse social fabric; and essential interests, including its critical infrastructure and governmental operations; and includes identifying and enabling the assessment of such threats". With the possible addition of wording such as "Such activities include, but are not limited to, terrorism, espionage, sabotage, violent extremism, insurrection, foreign interference, cyberthreats and serious transnational crime".

- Warrants authorising activities to contribute to New Zealand's international relations and well-being or economic well-being in respect of *non-New Zealanders* will continue to be assessed against the current criteria in s 60 and the criteria in s 61 of the ISA.
- The form of authorisation for the purposes of New Zealand's international relations and well-being and economic well-being would change in respect of New Zealanders, but this would not enlarge the scope for targeting New Zealanders.
- The authorisation framework will recognise the increasing use of data analytics to analyse bulk datasets, particularly for target discovery purposes.

Authorised activities and powers

No changes are suggested to the provisions of the ISA on authorised activities and powers.

Applications for warrants

- The ISA will more explicitly reflect the level of detail required in warrant applications.
- Applications will include the purpose of the warrant, the function to which it relates, the operational objective of the warrant, the activity proposed to be carried out under the warrant, and the grounds on which the application is made.
- Applications will include the arguments for and against the grant of the warrant, including any legal issues that arise in connection with the proposed warrant.
- Applications will include information relied on to justify the requirements of s 61 relating to necessity and proportionality, including the likelihood of third-party information being collected; and data retention, use and disposal requirements.
- Applications will include a statement that the Director-General confirms that all information relevant to the decision to issue a warrant that is known to the Agency has been set out in the application and is true and correct.
- Applications for a renewal or a repeat warrant will address why the authorisation should continue and the value of the information obtained under the previous warrant.

Duty of candour

- There is an express requirement to comply with the duty of candour in s 17 of the ISA.

Warrants targeting a class

- Applications may still be made in respect of an individual or individuals, or a class of persons.
- Where the application is for an authorisation in respect of a class of persons:
  - the class is defined with as much specificity as possible for the authorisation
  - information is provided on the particular characteristics that the persons in the class share or the common activities in which they are involved
  - the application sets out the process for confirming that an individual falls within the scope of the class, including the criteria to be used, and that this is necessary and proportionate
  - further policy work is undertaken with a view to potentially amending the ISA to more clearly identify when it is appropriate to determine that an individual fits within an existing class warrant or where it is appropriate to make a new, specific warrant application in respect of that individual.

Approval process

- Intelligence warrants are jointly approved by the authorising Minister and a Commissioner of Warrants.
- Commissioners of Intelligence Warrants will continue to be former High Court (or Court of Appeal, Supreme Court) judges, consistent with international best practice. Further policy work would be required to determine whether it is preferable for the role to be filled by sitting High Court judges.
- The functions of the Commissioners of Intelligence Warrants in s 114 are retained.
- Both issuers can impose restrictions and conditions on the authorisations.

Necessity and proportionality

- The application of the necessity and proportionality tests should be clarified in the ISA.
- The proposed activities authorised under the warrant must be necessary both for the s 9 purpose of the warrant and to fulfil a function of the Agencies.
- The activities under the warrant must be proportionate to the operational objective of the warrant.
- The proposed activities cannot reasonably be achieved by less intrusive means.
- The proposed activities must be rationally connected to the operational objective of the warrant.
- Satisfactory arrangements will be in place, to ensure that individual's expectations of privacy in personal information are taken into account.
- An assessment of necessity and proportionality applies at appropriate stages during activities authorised under a warrant, not simply at the point at which a warrant is issued.

Removal and practice warrants

- No changes are suggested to the provisions of the ISA on removal and practice warrants.

Urgent and very urgent warrants

- No changes are suggested to the provisions of the ISA on urgent warrants and very urgent authorisations, other than consequential amendments if the Type 1/Type 2 distinction is removed.

Reporting on intelligence warrants

- Information that must be maintained in the register of intelligence warrants under s 83 will include: the primary purpose under s 9 for which the warrant was issued, and the function under s 10, s 11 or s 12 to which the warrant relates.
- The annual reports of the Agencies will include information on the number of applications for intelligence warrants according to the primary purpose for which the warrant was sought, and where the purpose of the warrant is the acquisition of bulk datasets.
- To enhance transparency over bulk datasets, a requirement exists for a ministerial policy statement on the acquisition of bulk datasets.

Retention and disposal of information

- Information that is unintentionally obtained but is outside the scope of an authorisation or an authorised activity will be destroyed as soon as practicable, unless a further warrant (including an urgent warrant or very urgent authorisation) is sought or disclosure is made under s 104 of the ISA.
- What is and what is not "outside the scope of an authorisation" will be clarified.
- Information collected under warrant will be destroyed unless its retention is necessary both for a purpose for which a warrant may be granted and to fulfil the functions of an Agency.
- Information obtained under a warrant is reviewed at specified intervals to confirm that the justification for its retention is still valid.
- Information collected under warrant will be retained if necessary for oversight purposes, or, if it has been destroyed, then a record of this is kept.
- The necessity and proportionality tests will apply throughout the process of examination, use, retention and disposal of information.
- The applicable principles, policies and procedures for information retention and disposal will be made public to the greatest extent possible.

Appendix C
Routine improvements

Purpose

Throughout the course of the review, we received submissions on routine, minor and technical issues with the provisions in the Intelligence and Security Act 2017 (ISA). We also noted smaller issues in our own analysis of the ISA. These issues do not require in-depth analysis, and this appendix sets out our views and recommendations on these issues.

Definitions and interpretation

Change the definition of 'department' at section 4 of the Act

C.1. Section 4 of the Act defines 'department' as:

> Department—
>
> (a) means a department as defined in section 5 of the Public Service Act 2020; and
>
> (b) includes a departmental agency (as defined in that section) hosted by the department; and
>
> (c) includes an interdepartmental executive board (as defined in that section) serviced by the department.

C.2. Section 6 of the Public Service Act 2020 provides that a reference to department includes an interdepartmental venture, a departmental agency and an interdepartmental executive board. We recommend changing the s 4 definition of department in the ISA to explicitly align with s 6 of the Public Service Act 2020 by including reference to interdepartmental ventures.

Change the definition of 'employee' at section 4 of the Act

C.3. Section 4 of the Act defines 'employee' as:

> Employee, in relation to an intelligence and security agency, means a person employed in any capacity in that agency.

C.4. In line with the findings of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019,[696] we recommend expanding the definition of employee at s 4 to explicitly include secondees and contractors because this would more accurately reflect the staffing of the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) (the Agencies). In making this recommendation, however, we acknowledge that including 'contractors' in the definition creates some risk.

C.5. Contractors help the Agencies in a variety of legitimate ways, with temporary resourcing issues and access to particular skills, for example. However, significant outsourcing in relation to core

[696] Royal Commission of Inquiry *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) at part 8, chapter 14, [119].

functions can lead to the effective privatisation of security and intelligence functions, and a heightened risk of misconduct, insufficient transparency, accountability and oversight.

C.6. Mechanisms are in place to minimise this risk, and these may suffice. For example, the Public Services Act 2020, at Schedule 6, provides conditions on the delegation of functions or powers outside of the public service. Here, prior approval from the appropriate Minister is required before a chief executive can delegate a clearly defined function or power to a person outside the public service.[697] In addition, government procurement rules outline the government's standards of good practice for government procurement.[698]

Change the definition of 'agency' at section 22 of the Act

C.7. Section 22 of the Act defines 'agency' as:

> Agency includes—
>
> (a) a Minister; and
>
> (b) a statutory officer; and
>
> (c) a government agency; and
>
> (d) a private sector agency.

C.8. We recommend including 'foreign public agency' within the definition of agency at s 22. This would allow the Agencies to request help from foreign public agencies as required to enable the Part 3, Subpart 1 provisions of the Act. If this change is made, the foreign public agency will also have to adhere to its own legal framework if their help is requested.

Change the definition of 'counter-intelligence' at section 220 of the Act

C.9. Section 220 of the Act provides that any information obtained by the NZSIS for the purpose of a security clearance may only be used for the security clearance assessment, any other security clearance assessment and counter-intelligence.

C.10. Section 220 of the Act defines 'counter-intelligence' as:

> Counter-intelligence means the intelligence activities carried out to identify and counteract the threat, or potential threat, of unauthorised disclosure of official information by a person who holds, or has held, a New Zealand Government-sponsored national security clearance.

C.11. The above definition means information collected for an individual's initial application for a security clearance cannot be used for counter-intelligence because they do not currently hold, nor have they previously held, a national security clearance. Although individuals applying for their first security clearance will not have had access to New Zealand classified information, they may have had access to sensitive official information. We therefore recommend amending the definition of counter-intelligence at s 220 to include individuals applying for their initial security clearance.

---

[697] Public Services Act 2020, Sch 6, cl (2)(5).

[698] Ministry of Business, Innovation and Employment, *Government Procurement Rules: Rules for sustainable and inclusive procurement* (October 2019).

Ensure consistency between the purpose of the Act at section 3 and the functions of the agencies at section 17

C.12. Section 3(c) of the ISA provides that one purpose of the Act is "ensuring that the functions of the intelligence and security agencies are performed—

> (a) in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; and
>
> (b) with integrity and professionalism; and
>
> (c) in a manner that facilitates effective democratic oversight."

C.13. However, s 17 provides that "when performing its functions, an intelligence and security agency must act—

> (a) in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; and
>
> (b) in the performance of its operational functions, independently and impartially; and
>
> (c) with integrity and professionalism; and
>
> (d) in a manner that facilitates effective democratic oversight."

C.14. It is likely these two sections were intended to be the same. We recommend changing section 3(c) to include "in the performance of its operational functions, independently and impartially".

False or misleading representations

Provide former and prospective employees with the protections provided by section 228 and section 229 of the Act

C.15. Section 228 provides for employees of an Agency to make false or misleading representations to any person in connection to their employment for the purpose of keeping secret the fact that they are an employee of the Agency and in accordance with any requirements of the Director-General of the Agency. Section 229 provides corresponding immunities to that employee for providing false representations in accordance with s 228.

C.16. We recommend expanding s 228 and s 229 to also provide protections to former and prospective employees in relation to their employment with the Agency.

C.17. Additionally, we recommend changing the wording of s 228 to allow employees to make false or misleading representations regarding 'any employee' of the Agency.

Allow the agencies to request assistance from government agencies to support false or misleading representations made in accordance with section 228

C.18. To support their employees in maintaining the secrecy of their employment, the Agencies require the ability to provide documentation that supports false or misleading representations made in accordance with s 228.

C.19. We recommend providing the Agencies with the ability to request the assistance of New Zealand government agencies to support false or misleading representations. This could look similar to the provisions at s 25 that allow the Agencies to request assistance in relation to acquiring, using and maintaining assumed identities. However, it will require a specific legislative provision at s 228 and s 229, including the appropriate protections for the assisting agency.

Intelligence collection

Allow for ongoing section 121 requests

C.20. Section 121 provides for the Director-General of an Agency to request information from any other agency if they believe it is necessary to enable the Agency to perform any of its functions. The request must provide the details of the information requested and confirm that the information is necessary for the Agency to perform any of its functions.

C.21. It appears to be overly burdensome to require the Agencies to confirm that the information is necessary for it to perform any of its functions when the s 121 requests are ongoing or are follow-up requests for the same purpose.

C.22. We recommend amending s 121 to allow for ongoing requests or follow-up requests, without requiring further confirmation of necessity if the request is for the same purpose.

Allow for the collection of business records relating to employees of business agencies

C.23. The Agencies are able to request business records from telecommunications and financial service providers under the authority of a business records direction. However, the definition of 'business records' in s 144 (a)(ii)(A) and s 144(b)(ii)(A) excludes the "personal information about the network operator's or financial service provider's employees and directors". It is believed that the intent behind this exclusion was likely to prevent the Agencies from requesting human resourcing information or other information regarding employees from the business agencies under the authority of a business records direction. However, it also appears to prevent the Agencies from requesting the business record information outlined in s 144(a)(i) and s 144(b)(i) when the request is regarding an employee.

C.24. We recommend amending the exclusions at s 144(a)(ii) and s 144(b)(ii) to only limit the Agencies from requesting information beyond that specified in s 144(a)(i) and s 144(b)(i) respectively.

Increase the validity of approvals to obtain business records to 12 months

C.25. Section 148 provides that approvals to obtain business records expire 6 months after the date on which it is granted.

C.26. We have been unable to find any reasons for the 6-month time period, and we have not identified any issues with extending the length of these approvals to 12 months. Because the 12-month time period aligns with the maximum term for other authorisations in the ISA, such as intelligence warrants, we believe this is an appropriate duration for the approvals to obtain business records.

Require businesses responding to business records directions to maintain confidentiality

C.27. Currently, business agencies responding to a request under a business records direction are asked to be discreet about the requests they receive but they are not required to maintain confidentiality. We recommend that the business agencies be under an obligation of confidentiality in relation to the Agency requests. This would be a similar provision to s 108 that outlines an offence for unlawful use or disclosure of information in regard to authorised activities.

Duty of confidentiality

Allow individuals who are bound by the duty of confidentiality at section 219 to provide information to the review

C.28. Section 219 provides for a duty of confidentiality for any person who is, or has at any time been, appointed as: Inspector-General, Deputy Inspector General, Director-General of Security, Director-General of the GCSB, a member of the advisory panel, a person assisting the Inspector-General, a reviewer, or an individual employed by the Inspector-General or a Director-General. Unless otherwise authorised by the Minister responsible for an Agency that person must keep confidential all information that comes to their knowledge in the performance of their functions, duties or powers.

C.29. Section 237 provides for the provision of information to the periodic review. It allows the reviewers to request information, and be provided a response, from the current Directors-General and the Inspector-General. Section 237 does not provide for the reviewers to seek the opinions of, or information from, individuals who were previously in those roles, the Inspector-General's advisory panel, previous reviewers, unless ministerial authorisation is first sought.

C.30. We recommend expanding the application of the information-sharing provisions at s 237 to include all of the appointed positions listed in s 219. This would enable the review to independently contact and engage with all of the relevant individuals without requiring ministerial authorisation for each engagement.

Narrow the scope of the duty of confidentiality

C.31. As noted above, s 219 requires specified individuals to keep confidential all information that comes to their knowledge in the performance of their functions, duties or powers. We have been advised that the wide scope of this duty of confidentiality has created issues when individuals bound by the duty of confidentiality have wanted to share non-classified information that has come to their knowledge in the performance of their functions, duties or powers. This has included issues when employees of the Agencies have sought legal advice, engaged with other government departments, or sought employment outside of the Agencies.

C.32. We agree that instances occur when it would be appropriate for individuals bound by the duty of confidentiality to share non-classified information they have learnt in the performance of their functions, duties or powers. We recommend narrowing the scope of the duty of confidentially to all classified, operationally sensitive or information otherwise protected by legislation (Privacy Act 2020).

Oversight

Allow the Inspector-General of Intelligence and Security to transfer complaints to other oversight bodies

C.33. It is a function of the Inspector-General to deal with complaints received under s 171 of the ISA. While undertaking this function, the Inspector-General may consult with the Auditor-General, an Ombudsman, the Privacy Commissioner, a Human Rights Commissioner, the Independent Police Conduct Authority and the State Services Commissioner. The Act does not, however, provide for the Inspector-General to transfer a complaint to another oversight body.

C.34. We recommend including a provision in the ISA for the Inspector-General to transfer a complaint to another oversight body if they assess that another body is more appropriate to deal with the complaint, and they assess that the transfer of the complaint would not result in the inappropriate disclosure of sensitive information. This would be similar to provisions in the Ombudsmen Act 1975, which provides for the referrals of complaints to the Inspector-General.[699]

Require the Agencies to respond to the reports of the Inspector-General of Intelligence and Security in their annual report

C.35. Section 187 of the ISA provides that the Minister responsible for the relevant Agency must respond when provided a report from the Inspector-General in relation to an inquiry. This response must be provided to the Inspector-General and the Director-General of the relevant Agency. The Minister is not required to respond to other reports written by the Inspector-General, such as in response to a review. Any response from the Minister is also not required to be made public.

C.36. To help with transparency, we recommend requiring the relevant Agency to summarise in its annual report how it has responded to any Inspector-General reports that have been made public in that reporting year. This will provide the public with a better understanding of whether the Agencies agree or disagree with the reports of the Inspector-General, and whether they are planning on implementing any suggested changes.

Allow the Inspector-General of Intelligence and Security to conduct a review on their own initiative

C.37. Section 158 of the ISA provides the functions of the Inspector-General, and outlines the various circumstances in which the Inspector-General can undertake an inquiry or a review of the Agencies. Notably, the Inspector-General is able to conduct an **inquiry** at their own initiative into:

> (a) any matter relating to an Agency's compliance with New Zealand law, including human rights law;
>
> (b) any matter where it appears that a New Zealand person has been or may be adversely affected by an act, omission, practice, policy, or procedure of an Agency; and
>
> (c) the propriety of particular activities of an Agency.

C.38. However, while enabling the Inspector-General to initiate a broad range of reviews, the Act does not expressly provide for a self-initiated **review** of Agency activities that do not require an authorisation (such as the use of open-source information). While this has not so far prevented the Inspector-General reviewing such activities, we consider it would be preferable for the Inspector-General to have the power to self-initiate a less intrusive review to look into these kinds of activities, instead of requiring the initiation of a formal inquiry.

C.39. We recommend amending the functions of the Inspector-General to include an ability to self-initiate a review into any matter relating to an Agency's compliance with New Zealand law, including human rights and the propriety of particular activities of an Agency.

[699] Ombudsmen Act 1975, s 17C.

Amend the requirement for the Inspector-General of Intelligence and Security to return documents following an inquiry

C.40. Section 189 of the ISA requires the Inspector-General on completion of an inquiry, to return all information, documents and things relating to the inquiry that they obtained from the Agency. Because the Inspector-General is often provided information electronically, it is not always possible to 'return' the documents.

C.41. We recommend amending s 189 to require the Inspector-General to return or dispose of (in accordance with the requirements for the disposal of documents applying to the Agencies) information, documents and things relating to an inquiry that they obtained from the Agency. Additionally, the Inspector-General may retain information, documents and things if they are required to do so by legislation, including the Public Records Act 2005.

Additional policy work required

Assumed identities

Provide immunities for genuine companies established by an assumed identity

C.42. Section 24 of the ISA allows an employee to use an assumed identity to establish, maintain and operate a legal entity (with or without assistance under s 36 or s 37). However, if they establish a legal entity without the assistance of s 36 or s 37 that legal entity is not subject to the exemptions and immunities detailed in ss 42–44.

C.43. We recommend extending the exemptions and immunities detailed in ss 42–44 to also apply to legal entities established, maintained or operated by an assumed identity under Part 3. However, policy work will be needed to ensure the framework for these exemptions and immunities is fit for purpose.

Other issues raised

Provisions relating to Office of the Inspector-General

C.44. Section 11(4) of Schedule 3 of the ISA provides that an employee of the Office of the Inspector-General of Intelligence and Security "may not have access to any information in the possession of an intelligence and security agency except in accordance with the rules governing access to such information applying within the agency".

C.45. The Inspector-General has raised an issue with the review over the way this provision is being implemented and suggested clarification of it.[700] We have sympathy with the concerns of the Inspector-General. In general, access to information for oversight purposes should be facilitated, not hindered, by the Agencies. We do not consider that a legislative change is required. The Agencies should already be taking into account the context, requirements and needs of the Inspector-General's office when considering access to information by the Inspector-General's employees.

[700] This was also raised in the Inspector-General's 2022 annual report at p 3.

Intelligence collection

Should section 121(2) be removed from the Act?

C.46. Section 121 requests allow the agencies to request information from anyone on a voluntary basis. It does not require or compel the individual or group to provide the information. During the review, it was suggested that s 121(2) could be removed from the ISA. Section 121(2) provides that a request for information from the Agencies must:

> (a) provide details of the information requested; and
>
> (b) confirm that the information is necessary to enable the Agency to perform any of its functions.

C.47. It was put forward that the Agencies would always provide the details of the information required and would only ever ask for information necessary to enable its functions. Additionally, s 121 provides for an already lawful activity, therefore, s 121(2) is unnecessary.

C.48. However, we believe it is appropriate to retain s 121(2) in the ISA because it creates a requirement for the Agencies to actively consider whether the information they are requesting is necessary to perform its functions. This helps to create a control measure to prevent the agencies from requesting unnecessary or excessive information.

Should any employee of the Agencies be able to issue a section 121 information request?

C.49. Currently, s 121 may be issued by the Director-General of an Agency. This ability may then be delegated to specific employees and roles within the Agency. It was suggested that any employee of an Agency should be able to request information under s 121 because the section provides for an already lawful activity. If this was changed, the Directors-General would no longer be required to delegate this ability.

C.50. Although we are aware that the Directors-General are unlikely to see every s 121 request before they are made, we do believe the delegation process provides the Directors-General with a necessary level of oversight over the activities of their employees. It is also unlikely that every employee of the Agencies will need to request external information that is necessary to enable the Agency to perform any of its functions. It is therefore appropriate for the Directors-General to maintain control over which employees are delegated the ability to make these requests. We therefore assess that s 121 should remain unchanged.

Should the ISA and direct access agreements govern on-sharing of information?

C.51. It was suggested that the review may wish to consider whether the Agencies should be able to on-share information obtained through direct access in accordance with their objectives and functions, despite restrictions in the governing legislation of the agency holding the database. The review does not see the rationale for doing so because it may undermine the legitimate restrictions that Parliament intended to apply to certain information.