Office of the Inspector-General of Intelligence and Security

Submission of the Inspector-General of Intelligence and Security

on the Security Information in Proceedings Legislation Bill

Brendan Horsley
Inspector-General of Intelligence and Security
2 February 2022

Contents

INTRODUCTION

1. It will be well known to the members of the Committee that, when classified security information is used in proceedings, restrictions on access to that information must as far as possible be balanced with the rights of a non-State party to a fair trial and with long established principles of open justice and democratic accountability. Procedural fairness in administrative decision-making requires attempting a similar balancing. Of equal importance is that information/intelligence which may not be legitimately disclosed without causing prejudice to national security, for example, to its source or to a current intelligence and security agency operation, be appropriately protected during criminal and civil proceedings.

2. In these contexts, legislative safeguards for applicable procedure and decision-making take centre-stage. They can provide a measure of fairness when a person cannot hear and respond to the full information and allegations against them, when there is no 'equality of arms'. The Cabinet Paper preceding the Bill confirmed that the protections for security information were "a departure from the accepted principles of justice" and so the "protections for non-Crown parties are of the utmost importance".[1] As the Supreme Court of the United Kingdom held in *Al Rawi*,[2] closed procedures are such a departure from fundamental principles of fairness and open justice that they can not be developed by the common law.

3. The Bill gives rise to many connected and broad questions about the proposed statutory safeguards. For example, does the Bill unduly or unnecessarily constrain what the court can determine regarding disclosure of classified information? Does the Bill address the distinction between evidence and intelligence (the latter of which is often hearsay based and assessed for credibility and reliability according to its own system)? Can the special advocates function as necessary under the Bill as currently drafted – including considering whether the classified information suffers from the all too common problem of over-classification?

4. Striking the best balance is obviously a challenge, one that has been grappled with in Five Eyes jurisdictions and before the European Courts. Currently in the United Kingdom a review is underway of the operation of its Closed Material Procedures in civil proceedings under ss 6 to 11 of the Justice and Security Act 2013, with a submission to the review from all of the UK's special advocates making interesting reading.[3]

5. What coming to the issue now in New Zealand allows us to do is learn from the overseas experiences with handling such sensitive information and to aim for best practice in legislative

---

1 Minister of Justice, Hon Andrew Little, Cabinet Paper for Cabinet Social Wellbeing Committee *Managing National Security Information in Proceedings* (SWC-19-SUB-0191) at [25].

2 *Al Rawi and others v The Security Service and others* [2011] UKSC 34, [2012] 1 AC 531.

3 Review of Closed Material Procedures (CMP) pursuant to the Justice and Security Act 2013, s 13. The appointed reviewer of the operation of CMP in civil proceedings is Sir Duncan Ouseley. A 'call for evidence' was made between April and June 2021 and the reviewer's report is anticipated to be delivered to Parliament early in 2022 [Updated in April 2022 to be July 2022]. Terms of reference and other details are available at: www.gov.uk/guidance/review-of-closed-material-procedure-in-the-justice-and-security-act-2013. Two submissions to the review by all of the United Kingdom's special advocates are available at: www.ukhumanrightsblog.com/2021/06/27/secret-justice-the-insiders-view/ (a link) and at: www.ukhumanrightsblog.com/2021/14/12/secret-justice-review-the-special-advocates-respond-to-the-governments-submission/.

safeguards to be fully represented in this Bill. Indeed, the Cabinet Minute prior to the draft Bill stated that the proposals would "ensure that an appropriate balance is struck so that the rights of non-Crown parties are upheld to the greatest extent possible".[4] That balance has not been struck, as yet.

PERSPECTIVE OFFERED BY AN INDEPENDENT INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

6. Committee members may already be aware that my role, as Inspector-General of Intelligence and Security (IGIS),[5] is to carry out independent oversight of the two intelligence and security agencies, the New Zealand Security Intelligence Service and the Government Communications Security Bureau (together, "the agencies"). The Intelligence and Security Act 2017 ("ISA") requires my consideration of whether the broad range of the NZSIS' and the GCSB's activities, including those under intelligence warrants, are lawful and proper.

7. Much of the classified security information used in proceedings and being protected by this Bill is provided by these two agencies. Such information often establishes the basis for, by way of example, specific orders by the courts or recommendations for Ministerial decision-making. Business as usual for my office requires consideration of what best practice requires of the agencies when they provide such material, including whether available intelligence is included that may counter-balance negative information about an individual.

8. Such experience informs my assessment of the Bill's provisions and my views on whether the legislative safeguards are sufficient. I provide my recommendations on the legislation to Committee members with the need for a reasonable, best practice balance firmly in mind. As the United Kingdom's Supreme Court stated in *Al Rawi* and as repeated by the UK Joint Committee on Human Rights "radical departures from fundamental common law principles or other human rights principles must be justified by clear evidence of their strict necessity".[6]

9. Further, the Law Commission's *Report*[7] of its review of security information, which significantly underpins this Bill, recommended that the oversight powers of the Inspector-General be better integrated into the context of national security information when it assists with administrative decision-making.[8] In terms of remedies, an obvious benefit of IGIS engagement through, for example, the investigation of complaints, is that it comes at no cost to a complainant (in contrast to, for example, judicial review).

---

4 Cabinet Social Wellbeing Committee Minute *Managing National Security Information in Proceedings* (SWC-19-MIN-0191) at [7.4].

5 IGIS' Annual Reports; Work Programme and Inquiry and Review Reports are available at: www.igis.govt.nz.

6 *Al Rawi and others v The Security Service and others* [2011] UKSC 34, [2012] 1 AC 531; United Kingdom House of Lords and House of Commons Joint Committee on Human Rights *Legislative Scrutiny: Justice and Security Bill: Fourth Report of Sessions: 2012-13* HL Paper 59 HC 370 (13 November 2012) at [17].

7 New Zealand Law Commission *The Crown in Court: A review of the Crown Proceedings Act and national security information in proceedings* (NZLC, R135, 14 December 2015).

8 NZLC *The Crown in Court: A review of the Crown Proceedings Act and national security information in proceedings* (NZLC, R135, 14 December 2015) at 152, Recommendations 20 to 23.

SUMMARY OF RECOMMENDATIONS OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

10. Committee members will find the reasoning for my recommendations in the body of my submission. I primarily address the Bill's provisions that relate to civil proceedings and administrative decision-making.

Recommendation A: I recommend that the Terrorism Suppression (Control Orders) Act 2019 be amended by adding a notification clause to the Bill, providing for the following:

> The Director-General of an intelligence and security agency must notify the Inspector-General of Intelligence and Security if the agency provides classified information to the Commissioner of Police or to the New Zealand Police to assist the Commissioner to decide whether to make an application under the Terrorism Suppression (Control Orders) Act 2019 for:
>
> a. a control order under section 14;
> b. the renewal of a control order under section 26; or
> c. the variation or discharge of a control order under section 27.
>
> The Director-General must make the notification as soon as practicable after providing the classified security information to assist the Commissioner.

Recommendation B: I recommend that the Outer Space and High-altitude Activities Act 2017 be amended by this Bill, to add the following notice provision to that Act:

> The affected party may be able to make a complaint to the Inspector-General of Intelligence and Security under section 171 of the Intelligence and Security Act 2017 in relation to any advice given to the decision-maker by an intelligence and security agency.

Recommendation C: I recommend that clause 19 of the Bill be amended so the court may allow the special advocate to make submissions in both the open and the closed hearings of a specified proceeding, as follows:

> The role of a special advocate is to act in the interests of the specially represented party for the purposes ~~of the closed hearing~~ of the specified proceeding.

Recommendation D: I recommend that special advocates be allowed to fulfil their intended role, by deleting clause 12(3) of the Bill which can limit the special advocate's access to *all* of the security information at issue.

Recommendation E: I recommend the Bill be amended by adding a clause requiring the development of a guiding protocol on the use of the NSI certificate process (with the protocol presumably to be developed by the agency that administers this legislation). The clause will also set out that the protocol must include:

a. a requirement that the Crown use the NSI certificate process as a last resort with the default being the court as decision-maker;

b. a threshold similar to 'exceptional circumstances' before the certificate process is engaged; and

c. criteria for the detail that the applicant (on the SI application) and the certificate issuers (on the certificate) are to provide.

Recommendation F: I recommend that the Bill be amended to add a requirement for a periodic review of its operation, scheduled to occur five years after the Bill comes into force.

ENSURING EFFECTIVE OVERSIGHT OF INTELLIGENCE AGENCIES: NOTIFICATION TO IGIS: NOTICE TO AFFECTED PARTY

13. During the development of the Cabinet Papers and Bill, my office provided the Ministry of Justice with several rounds of substantive comment, in particular with regard to IGIS notifications. This focus, in part to implement Law Commission recommendations, required amendments to other legislation to ensure that:

    13.1. The Inspector-General receives **notification** from the Director-General of an intelligence and security agency when the agency has contributed classified security information to assist decision-makers with regard to specific administrative decisions or in relation to civil proceedings; or

    13.2. A potentially affected party receives **notice** of their ability to make a complaint to IGIS about the actions of an intelligence and security agency where a relevant decision by another Minister/body relied on classified security information.

14. The principles[9] that distinguish situations where notification to IGIS is appropriate, as opposed to where direct notice of the IGIS' complaints function to a party is appropriate, are as follows:

    14.1. **Notification**: As the Law Commission stated, this requirement is engaged when administrative decisions, or applications for civil proceedings, are made in reliance on national security material and, importantly, where those decisions affect individual rights; there is a strong likelihood that a potentially affected person will be unaware of the intelligence and security agencies' role in the decision made and therefore unaware that a complaint to IGIS is possible or even how to frame that complaint; it is unlikely that, without notification, the Inspector-General will be aware of the intelligence agencies' contributions to each of these administrative decisions/applications; such decisions arise infrequently so the volume of required notifications is likely to be strictly limited and thus not onerous for the agencies and manageable under IGIS resources; and, critically, upon notification the IGIS is able to determine whether the intelligence and security agencies' actions/contribution to the decision-maker – which may in any one instance be broader than with regard to providing classified information – merits further IGIS inquiry.

    14.2. **Notice**: This requirement is engaged where, due to other provisions in the relevant enactments, a party such as a telecommunications service provider or person seeking to launch a high altitude vehicle, for example, will be aware that contributions are being made by the intelligence and security agencies to relevant decisions, including that the agencies' contribution likely involves classified security information; this means that adding a direct complaints notice to the enactment will not disclose that the intelligence and security agency had a role. The clause in the Bill should address the particular type of information and/or the particular role the intelligence agencies occupy in relation to the decision, to enable the potentially affected party to focus any complaint made to IGIS. Under ISA ss 171 to 174 the Inspector-General is able to assess the merits or otherwise

9 As IGIS advised to Ministry of Justice officials, by letter to MoJ (6 November 2020).

of a complaint, meaning it is not necessary for any such qualifiers to be included in this Bill.

Notifications to IGIS: Add to Terrorism Suppression (Control Orders) Act 2019

15. During the development of the Bill the intelligence and security agencies and I came to an agreement on the form of words for notifications to the Inspector-General of Intelligence and Security, in circumstances in keeping with the above principles. The Bill adds IGIS notification clauses through amendments to the Passports Act 1992[10], regarding passport revocations, and to the Terrorism Suppression Act 2002, regarding designations of terrorist or associated entities.[11] The form of words for the notifications is along the following lines:

> The Director-General of an intelligence and security agency must notify the Inspector-General of Intelligence and Security if the agency provides classified information to the [Minister/Prime Minister] or department to assist the [Minister/Prime Minister] to decide whether to ...[12]

16. The Director-General must make the notification to the IGIS "as soon as practicable after providing the classified security information …". I consider this a positive development, ensuring the "facilitation of effective oversight", in particular for these infrequent activities by the agencies, on matters not immediately visible to oversight and which may significantly impact upon an individual's rights.[13]

17. However, legislation introducing the use of control orders into New Zealand – the Terrorism Suppression (Control Orders) Act 2019 – was enacted some four years after the Law Commission's report on national security information in proceedings. Hence the Commission's recommendations did not address that Act in relation to proposed safeguards, including those provided by oversight.

18. Nevertheless both the NZSIS and the Ministry of Justice have flagged, respectively to Parliament and to the Government, that the scheme being developed for security information and now presented in this Bill could cover control orders. The Service's advice to Select Committee on the control orders legislation[14] stated that "[t]he Ministry of Justice is developing a process to manage national security information in court proceedings. Control orders will be covered by this new process". The 2019 Cabinet Paper[15] also identified legislative regimes established post the Law Commission's report, including for control orders, that might benefit from measures

---

10 Security Information in Proceedings Legislation Bill clause 87, adding new s 27GFA into the Passports Act 1992.

11 SIPL Bill clause 119, adding new s 31A into the Terrorism Suppression Act 2002.

12 A specific point the IGIS focused upon, in agreeing to this form of words with the intelligence and security agencies, was that there was no requirement for the classified information to have been provided to the decision-maker *for the purpose* of the specific decision, as this is too narrow a description to ensure effective oversight. In my experience, it can be the case that the contribution of an intelligence and security agency is made for another or an incidental purpose but the contribution subsequently assists a decision of a type referenced under this Bill.

13 This is a requirement of the intelligence and security agencies under ISA ss 3(c)(iii) and 17(d).

14 NZSIS *Advice to the Foreign Affairs, Defence and Trade Committee: Terrorism Suppression (Control Orders) Bill* (14 November 2019; Unclassified) at [22].

15 Cabinet Social Wellbeing Committee *Managing National Security Information in Proceedings* (SWC-19-SUB-0191) at [18].

relating to security information, such as a closed court process.[16] In my view, there is benefit to such measures including a clear nod towards independent oversight, with notification aiding my ability to deliver consistent oversight in the public interest.

Recommendation A

Recommendation A: I recommend that the Terrorism Suppression (Control Orders) Act 2019 be amended by adding a notification clause to the Bill, providing for the following:

> The Director-General of an intelligence and security agency must notify the Inspector-General of Intelligence and Security if the agency provides classified information to the Commissioner of Police or to the New Zealand Police to assist the Commissioner to decide whether to make an application under the Terrorism Suppression (Control Orders) Act 2019 for:
>
> a. a control order under section 14;
> b. the renewal of a control order under section 26; or
> c. the variation or discharge of a control order under section 27.
>
> The Director-General must make the notification as soon as practicable after providing the classified security information to assist the Commissioner.

Notice to potentially affected party regarding IGIS complaints function: Add to OSHAA

20. The Bill amends the Telecommunications (Interception Capability and Security) Act 2013 (TICSA)[17] by adding a notice provision. This advises a potentially affected party of their ability to lodge a complaint with the Inspector-General of Intelligence and Security.

21. However, such a notice provision is absent from the amendments to the Outer Space and High-altitude Activities Act 2017 (OSHAA).[18] In April 2021 I carried out a review of the GCSB and NZSIS activity and assessments under OSHAA. The Public Report of my review, available on the IGIS website,[19] examined the way in which the agencies support their Minister by conducting national security risk assessments of applications for licences or permits under the Act. Given the agencies role, it is appropriate that OSHAA direct potentially affected persons to the IGIS complaints function – there may be people, for example, who have not received a sought licence on the basis of the agencies' security risk assessment.

22. It is for Parliamentary Counsel to identify the best placement of this clause in OSHAA.

---

16 The Cabinet Paper cited the Outer Space and High-altitude Activities Act 2017 and the (then) Terrorism Suppression (Control Orders) Bill, amongst others.

17 See SIPL Bill 2021 clause 99, adding new s 44B(1)(c) to TICSA.

18 See SIPL Bill 2021 clauses 147 and 148 re the OSHAA.

19 Available at www.igis.govt.nz/Publications/IGISReports.

Recommendation B

Recommendation B: I recommend that the Outer Space and High-altitude Activities Act 2017 be amended by this Bill, to add the following notice provision to that Act:

> The affected party may be able to make a complaint to the Inspector-General of Intelligence and Security under section 171 of the Intelligence and Security Act 2017 in relation to any advice given to the decision-maker by an intelligence and security agency.

SECURE AN APPROPRIATE ROLE FOR A SPECIAL ADVOCATE

23. The United Kingdom's Supreme Court stated that the special advocate system is:[20]

> [A] distinctly second best attempt to secure a just outcome to proceedings. It should always be a measure of last resort, one to which recourse is only had when no possible alternative is available. It should never be regarded as an accepted substitute for the compromise of a fundamental right.

24. Further, in its assessment of this Bill, Crown Law advised the Attorney-General that "an important mitigation for this limitation of rights is the special advocate procedure".[21] The emphasis is therefore upon the role of the special advocate being set out in this Bill in a manner that provides best practice in a difficult context.

25. My interest in ensuring best practice in this regard arises in two ways, both connected to the oversight of the intelligence agencies.[22] The first is the special advocate's ability to deliver benefit in both the open and closed hearing of a matter – to assess and address in submissions, as necessary and appropriate, the balance, relevance and accuracy of the Crown's submissions in open court, when premised on the classified security information only disclosed in closed proceedings. The second is the role of the special advocate in submitting to the court where security information, despite its classification might be disclosable in open court – in other words, where the security information may prove to be over-classified.

26. An eminent United Kingdom special advocate, Nick Blake QC, explained the special advocate's performance of their function – to promote the interests of the appellant – in two ways:[23]

> First, they seek to maximise disclosure to the individual concerned, by looking at the closed case to see whether there is anything which could be open material and also at what is not before the … court but which should be, such as exculpatory material, further investigations or other material which might tend to undermine the hypothesis against

---

20 *Al Rawi and others v The Security Service and others* [2011] UKSC 34, Lord Kerr at [94].

21 Crown Law letter to Attorney-General "Security Information in Proceedings Legislation Bill [PCO22599/11.8] – Consistency with the New Zealand Bill of Rights Act 1990" (30 September 2021) at [25].

22 My office, with the approval of the Court has observed the open and closed proceedings in *A v Minister of Internal Affairs*, a judicial review of passport revocation, and has done so in both the High Court and recent Court of Appeal hearings.

23 United Kingdom House of Lords and House of Commons Joint Committee on Human Rights *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning; Nineteenth Report of Session 2006-07* HL Paper 157 HC 394 (30 July 2007) at [191].

> the individual concerned. Second, Special Advocates test the hypothesis against the person in the closed proceedings.

The potential over-classification of security information

27. In *A v Minister of Internal Affairs* Dobson J stated that, at previous stages in the case, the special advocate had "made submissions challenging the extent to which the respondent has claimed to withhold discoverable documents from the applicant on the grounds that it is CSI".[24] This reflects the practical comments of the United Kingdom special advocate cited above on the usefulness of the advocate's role in identifying what may be over-classified material. It also reflects the Law Commission's view that the scrutiny the special advocate brings to hearings "should assist in addressing concerns that material may be unjustifiably claimed to be national security information".[25]

28. Classification is a key tool to appropriately protect security material but, as with any such protection, it requires cautious application and robust justification. In my experience, over-classification is a real and present concern.[26] My office conducted a review of the New Zealand Security Classification System in September 2018 and proposed a simplified system, stating at that time that the over-classification of documents is "an inherent vice of security classification systems".[27]

29. Further, the *Procedural protocol* adopted by the 2019 Government Inquiry into Operation Burnham stated:[28]

> As has occurred in other inquiries and in court proceedings in New Zealand and elsewhere, the Inquiry anticipates that some classifications may be overbroad, outdated, overtaken by disclosures that have already occurred or outweighed by contrary public interest considerations favouring disclosure. It is expected that the review process, with the full and prompt cooperation of the parties seeking to withhold information from disclosure, will provide an efficient way to progress such material.

30. It is prudent to assume that some of the classified security information at issue in civil proceedings and administrative decision-making may suffer from such issues and benefit from the consideration a special advocate can afford to it.

31. Notwithstanding the role of the special advocate, in light of the long-standing principle of open justice, I wish to stress that it is appropriate for a Crown party to take the initial responsibility for maximising open disclosure.

---

24 *A v Minister of Internal Affairs* [2019] NZHC 2992, at [6] and footnote 2. (CSI is classified security information.)

25 New Zealand Law Commission (NZLC, R135, December 2015) at [9.26] to [9.27].

26 I am on the public record regarding this issue, most recently: "On the whole I think the balance between transparency and legitimate classification concerns is still slightly skewed towards over-classification. … There are areas where I think more consideration could be given to disclosing activities for the benefit of informing the public. Over-classification is the enemy of transparency." Laura Walters "Cameras in the shadows: when NZ spy agencies test public trust" *The Spinoff* (1 July 2021). I published similar comment in the Forewords to IGIS Annual Reports in 2020 and 2021 at 2 and 1 respectively: noting that "the over-classification of information is a barrier to public understanding and scrutiny".

27 IGIS "A review of the New Zealand Security Classification System" (September 2018) at [242].

28 Government Inquiry into Operation Burnham and Related Matters *Procedural protocol for review of classified information / claims to withhold information from disclosure* (20 February 2019) at [4].

Special advocate's submissions of assistance in open and closed hearings

32. My office has closely observed the special advocate process in action in New Zealand, attending the open and closed hearings in *A v Minister of Internal Affairs*,[29] both in the High Court and more recently in the Court of Appeal.[30] Committee members may be aware that, as a preliminary matter in the High Court, the Crown challenged whether it was "appropriate" for the special advocate to "make submissions during open court hearings where the applicant is representing their own interests".[31] The Court was not persuaded to limit the role of the special advocate in the manner submitted by the Crown.

33. Rather, Dobson J addressed the scope of involvement by the advocate "as a matter for the Court to direct" and was willing to "afford the special advocate a brief opportunity to respond to matters raised in relation to the content of his written submissions, and new matters that had not been addressed in them".[32] As we observed the hearings, we are aware that the advocate subsequently made substantial submissions in both the closed and open hearings, a practice repeated in the recent Court of Appeal hearing. In such hearings, I consider it important that the intelligence and security agencies' classified information is subjected to, and can withstand, an appropriate level of rigour.

34. The High Court judgment also reflected the continued usefulness of the special advocate's submissions during the open hearings, with Dobson J stating that:[33]

> The scope of those arguments [against the passport cancellation] was conveyed to her in advance of the open hearing by Mr Keith [the Special Advocate] presenting a redacted form of his full submissions ... Ms A observed all of the argument during the open hearing and endorsed all of the arguments made in support of her case by Mr Keith.

35. One example of the difficulty and lack of fairness that could arise if the Bill restricts the special advocate to submitting to the court in closed hearings only is as follows: Should the Crown claim in an open hearing that an argument is supported by the closed material, the party excluded from the closed hearing and their counsel will hear that claim but have no information against which to assess it, and the special advisor will have the information enabling such an assessment to be made, but will not be able to submit that view to the court in the open proceedings with the non-Crown party present.

36. While New Zealand experience is to date constrained to several cases,[34] there is support in other jurisdictions for the current position adopted by the New Zealand judiciary, namely, that the submissions of a special advocate can be relevant and useful in both closed and open hearings. In Canada, for example, while the Immigration and Refugee Protection Act 2001 referenced the role of the special advocate in relation to closed hearings, by 2014 Canada's Supreme Court in

---

29 *A v Minister of Internal Affairs* [2020] NZHC 2782.

30 I considered this oversight to be appropriate, due to the significant involvement of an intelligence and security agency in this matter.

31 *A v Minister of Internal Affairs* [2019] NZHC 2992 at [6].

32 *A v Minister of Internal Affairs* [2019] NZHC 2992, at [6] and [8].

33 *A v Minister of Internal Affairs* [2020] NZHC 2782, at [22].

34 *A v Minister of Internal Affairs* [2019] NZHC 2992, at [24]; "A range of novel legal issues have arisen in what is the first proceeding under the relevant statutory provisions to reach the present stage." In *Dotcom v Attorney-General* [2019] NZCA 412, the Court of Appeal appointed special advocates under its inherent jurisdiction who made submissions in both the open and closed hearings.

Canada (Citizenship and Immigration) v Harkat clearly contemplated a role for the special advocate in an open hearing:[35]

> The open court principle is a 'hallmark of a democratic society and applies to all judicial proceedings'.[36] 'National security does not negate the open court principle'.[37] … The issues in this appeal do not turn on confidential information and could have been debated fully in public without any serious risk of disclosure, supplemented where necessary by brief closed written submissions and by the closed record. The special advocates could have been given judicial permission to make public submissions, so long as they refrained from disclosing confidential information.

Recommendation C

Recommendation C: I recommend that clause 19 of the Bill be amended so the court may allow the special advocate to make submissions in both the open and the closed hearings of a specified proceeding, as follows:

> The role of a special advocate is to act in the interests of the specially represented party for the purposes ~~of the closed hearing~~ of the specified proceeding.

Special advocate's access to all security information at issue

37. The Cabinet Paper that preceded the Bill advised Ministers that "the special advocate would have full access to the NSI [national security information] at issue in the proceedings".[38] The Paper for the Cabinet Legislation Committee reiterated that "under a closed procedure a special advocate would be able to view the security information".[39] Further, the Minister of Justice's Press Release[40] when the Bill was introduced into the House repeated that the special advocate "would have full access to the national security information". The Bill, however, has not delivered on this undertaking. It seems unlikely a special advocate can sufficiently carry out their role without access to the *full* security information at issue. Further, I suggest the Bill should make it clear that the special advocate will be provided with a copy of the Crown's SI (Security Information) application in civil proceedings.[41]

38. I question the necessity or advisability of a court (presumably on submission from the Crown) constraining a special advocate's access to this information. This is particularly given the special advocate is appointed from a panel of lawyers with "suitable knowledge and experience",[42] holds an appropriate security clearance, and will be acting under specific statutory obligations of confidentiality.[43]

---

35 *Canada (Citizenship and Immigration) v Harkat* [2014] 2 SCR 33 at [24] to [25].
36 *Vancouver Sun (re)* [2004] 2 SCR 332 at [23].
37 Craig Forcese *National Security Law: Canadian Practice in International Perspective* (2008) at 402.
38 Cabinet Social Wellbeing Committee *Managing National Security Information in Proceedings* (SWC-19-SUB-0191) at [36.3].
39 Cabinet Legislation Committee *Security Information in Proceedings Legislation Bill: Approval for Introduction* (2021) at [36].
40 Hon Kris Faafoi Minister of Justice Press Release (25 November 2021).
41 Clause 32 of the SIPL Bill refers.
42 Clause 16 of the SIPL Bill refers.
43 See clauses 21, 22 and 26 of the SIPL Bill.

Recommendation D

> **Recommendation D:** I recommend that special advocates be allowed to fulfil their intended role, by deleting clause 12(3) of the Bill which can limit the special advocate's access to *all* of the security information at issue.

Training and support for special advocates

40. While I do not intend to make a recommendation on matters of training and support, Committee members may wish to consider whether the Bill would be strengthened by requirements to assist special advocates in their potentially difficult task.

41. A submission in June 2021 from all the United Kingdom's special advocates,[44] to the Ouseley Review currently underway of closed material procedures, sets out the special advocates' experience of "serious failures" with the government's provision of training and support. The special advocates recommend:

    41.1. Training – Increased training made available by the government where required by the advocate;

    41.2. Support – for example, to cover the cost of independent junior legal support for the special advocate; the provision of dedicated facilities (ie, access to space in a Sensitive Compartmentalised Information Facility (SCIF)) for special advocates to work with classified security information; and/or access to a database of closed judgments.

THE NSI CERTIFICATE PROCESS: THE ROLE REMAINING TO THE COURT: LACK OF SAFEGUARDS IN CERTIFICATE PROCESS AS DRAFTED

42. I question the necessity for a national security information (NSI) certificate process, as set out in clauses 41 and 42 of the Bill. However, presuming this process remains in the Bill, I consider the certificate process as currently drafted to be inadequate – in my view it does not require sufficient accountability from the Crown. The Cabinet Paper[45] prior to the Bill indicated the certificate process was justified on the grounds of "a need for a greater level of certainty", where some security information is "so sensitive it requires this level of protection" that it will not be disclosed. In my view, this is a category of security information where it would surely be straightforward to apprise the court of its sensitivity, of its "greater need" for protection, when making an application to the court for an NSI order. This begs the question of why the certificate process is required.

43. As now drafted in the Bill, my concern is first that it circumvents the court as the competent and consistent decision-maker on what comprises security information for the specified proceedings. The only option left for the court is the nature of the (now limited) orders it might

---

44 See details above at note 3.

45 Cabinet Social Wellbeing Committee *Managing National Security Information in Proceedings* (SWC-19-SUB-0191) at [42].

make with regard to the security information. Secondly, I am concerned at the lack of safeguards in the certificate process, where an NSI certificate is sought from the Attorney-General and the Minister of Foreign Affairs (MFA).

The role remaining to the court

44. As Dobson J observed in *A v Minister of Internal Affairs*, in respect of the court's role in a closed court procedure under the Passports Act 1992:[46]

> The whole of our common law tradition, as bolstered by the rights and protections recognised by NZBoRA, render the procedure under s 29AB [of the Passports Act] an anathema to the fundamental concepts of fairness. However, the reality is that Parliament has recognised the justification for use of that procedure in defined circumstances. … The task of the court is to apply statutory provisions consistently with the interpretation of such [NZBoRA] provisions as discerned by the courts.

45. The European Court of Human Rights has emphasised the importance of allowing a trial judge to rule on questions of disclosure.[47]

46. Committee members will be aware that the NSI certificate was not a mechanism recommended by the Law Commission. The Cabinet Paper prior to the Bill included that:[48]

> In 2015, the Law Commission consulted the judiciary on its recommended approach. The then-Chief Justice, on behalf of the Senior Courts, supported the court being the ultimate decision-maker on the treatment of NSI before the courts as the only effective way of ensuring there is a check on Executive power.
>
> The proposal to have a process involving a certificate removes some of the court's decision-making ability. Accordingly, I also consulted the Chief Justice before bringing these proposals to Cabinet. The view of a sub-committee of the Legislation and Law Reform Committee of the judiciary was supportive of the Law Commission's proposal. … The sub-committee also questioned the utility of the certificate process.

47. I tend to agree with the considered views expressed by the Law Commission and the judiciary, on the role of the courts as the appropriate decision-makers regarding NSI in proceedings.

Lack of safeguards in the certificate process as drafted

48. The Cabinet Paper informed Ministers that the use of the certificate process would be "rare", and that:[49]

> [T]o ensure the certificate option is reserved for exceptional cases where information is so sensitive it requires this level of protection, I consider that safeguards are required to prevent the certificate process from becoming the default option.
>
> I propose that under a protocol, the Crown would be required to consider the non-certificate track first and that this would be reflected in advice to certifying Ministers. I

---

46 *A v Minister of Internal Affairs* [2017] NZHC 746 at [84].

47 See for example *Rowe and Davis v the United Kingdom* ECtHR Application No 28901/95 Judgment of 16 February 2000; *Dowsett v the United Kingdom* ECtHR Application No. 39482/98 Judgment of 24 June 2003.

48 Cabinet Social Wellbeing Committee *Managing National Security Information in Proceedings* (SWC-19-SUB-0191) at [78] and [79].

49 Cabinet Social Wellbeing Committee *Managing National Security Information in Proceedings* (SWC-19-SUB-0191) at [42], [46] and [47].

> also propose that an application by the Crown under the non-certificate track would preclude the use of the certificate track.

49. I appreciate that this advice is predicated on the creation of a 'protocol'. My assessment is that such an official procedure is too important to be completely absent from the Bill. The requirement for a guiding protocol, accompanied by an in-exhaustive note of its requisite contents, should be signaled at high level in the legislation.

50. Such a statutory safeguard will promote effective oversight, by providing a primary benchmark against which to consider the actions of the agencies in the contexts addressed by the Bill. Further, without this clear safeguard, there is limited protection for the integrity of the process – it will be invisible to the New Zealand public. The Crown Law assessment of the Bill for compliance with the New Zealand Bill of Rights Act 1990, which *is* publicly available, noted:[50]

> There is no guidance in the Bill as to which track [certificate or non-certificate] is to be used when, so it gives a broad discretion to the Crown to choose the track. There is no appeal procedure for a certificate but judicial review of a certificate would be possible. …
>
> Further, the certificate track can be used at the discretion of the Crown; there is no restriction on when it can be used.

Recommendation E

Recommendation E: I recommend the Bill be amended by adding a clause requiring the development of a guiding protocol on the use of the NSI certificate process (with the protocol presumably to be developed by the agency that administers this legislation). The clause will also set out that the protocol must include:

a. a requirement that the Crown use the NSI certificate process as a last resort with the default being the court as decision-maker;

b. a threshold similar to 'exceptional circumstances' before the certificate process is engaged; and

c. criteria for the detail that the applicant (on the SI application) and the certificate issuers (on the certificate) are to provide.

PERIODIC REVIEW OF THE OPERATION OF SECURITY INFORMATION IN PROCEEDINGS LEGISLATION

51. A scheduled review provides an overarching legislative safeguard, given the importance of ensuring the Bill has struck a workable balance between protecting security information in proceedings and in administrative decision-making, and protecting – as far as possible – the human rights of participants in the justice system. The Law Commission may be an appropriate body to undertake such a review.

---

50 Crown Law letter to Attorney-General "Security Information in Proceedings Legislation Bill [PCO22599/11.8] – Consistency with the New Zealand Bill of Rights Act 1990" (30 September 2021) at [7] and [24].

52. Committee members may be interested to observe that the current review underway in the United Kingdom, of the closed material procedures under the Justice and Security Act 2013, is by virtue of a statutory requirement for a five-yearly review of the Act's operation.

Recommendation F

> **Recommendation F:** I recommend that the Bill be amended to add a requirement for a periodic review of its operation, scheduled to occur five years after the Bill comes into force.

PUBLICATION OF IGIS SUBMISSION

54. Lastly, in accordance with Standing Order 221, I wish to advise Committee members of my intention to publish my submission, on the IGIS website on the day of my appearance before the Committee.