Office of the Inspector-General of Intelligence and Security

Best Practice Approaches To Information Sharing and Cooperation: Ensuring Lawful Action (from the Inquiry's classified Report)

Supplementary Paper

To the Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001-2009

Cheryl Gwyn
Inspector-General of Intelligence and Security
31 July 2019

BEST PRACTICE APPROACHES TO INFORMATION SHARING AND COOPERATION: ENSURING LAWFUL ACTION

Introduction

1. The classified version of the Inquiry Report contained an extensive survey and analysis of the elements of best practice in the field of information sharing with foreign partners. In comparison, the Public Report of the Inquiry (Public Inquiry Report) contained a brief discussion of that material and a summary of the principal elements of best practice. For those who have a deeper interest in the issues relevant to best practice, this supplementary paper makes available the full section on best practices from the classified Inquiry Report.

Benefits from observing best practice

2. As identified in the Inquiry Report, some difficult practical questions arise in the context of intelligence-sharing arrangements, particularly in routine and reciprocal relationships between intelligence and security agencies, given that the law relating to complicity in torture is complex and far from settled.[1] The likelihood of States being held responsible for the actions of officials sharing or using information obtained by torture as part of systematic and mutual information sharing arrangements between States is relatively untested. What is clear, however, is that no part of that exchange process can properly be described as "passive." In effect, the exchange of information is the currency of the relationship.

3. New Zealand intelligence and security agencies are net beneficiaries of information sharing and co-operation with foreign partners, and with the Five Eyes partners in particular.[2] These relationships are highly valued and New Zealand is keen to preserve them, alongside developing other connections. However, New Zealand and overseas experience to date demonstrates that relying on relationships of trust, and personal assurances provided at high level by foreign States and agencies, are not sufficient to guarantee compliance with international and domestic law.

4. The Inquiry Report demonstrates the various legal, political and practical complexities that New Zealand's intelligence and security agencies have to navigate, in sharing information and cooperating with foreign States and agencies, to ensure the actions of New Zealand agencies are legally compliant. This best practice section (drawn from the classified Inquiry Report) proposes that the prudent and precautionary approach is to observe requirements to exercise due diligence[3] and adopt a best practice approach to both policy and operational practice. Measures must provide a margin of safety, be effective and apply across agency functions. They need to be relevant to instances where there is an established intelligence relationship as well as where the connection with the foreign authority is ad hoc, one off, or infrequent.

---

1 See Appendix D of the Public Inquiry Report.

2 Sir Michael Cullen and Dame Patsy Reddy *Intelligence and Security in a Free Society* (9.24a, February 2016) (Cullen and Reddy) at [3.43] and [3.47].

3 See the discussion of due diligence in Anja Seibert-Fohr "From Complicity to Due Diligence: When do States Incur Responsibility for Their Involvement in Serious International Wrongdoing?" German Yearbook of International Law, (2018) (60) (Forthcoming) at 11 - 19.

5. A key purpose of best practice requirements is to achieve greater consistency among States and agencies that cooperate on intelligence and security matters, to ensure human rights obligations are engaged and respected as part of everyday practice.[4] The following paragraphs survey what are commonly recognised as, and what I consider to be, the best practice requirements for a sound policy and legal framework for information sharing and cooperation by intelligence and security agencies. A summary of the elements of best practice is included at the end of this Part of the Report.[5]

ELEMENTS OF BEST PRACTICE

Ministerial Directions: Provide high-level regulation and guidance

New Zealand: 2017 Ministerial Policy Statement

6. The ISA in 2017 established Ministerial Policy Statements (MPSs) as:

- "a mechanism to enable the responsible Minister to regulate the lawful activities of the agencies";
- "to enhance oversight and compliance"; and
- "to ensure the agencies have clear and objective guidance about how they are to carry out their lawful activities".[6]

7. The MPSs provide guidance to the intelligence and security agencies in relation to ten stated areas.[7] Relevant to this Inquiry, the Ministerial Policy Statement on *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities* (MPS Overseas Cooperation) sets out procedures to authorise intelligence cooperation, assistance and sharing, and the protections and restrictions that need apply. The MPS Overseas Cooperation took effect from 28 September 2017 for three years, unless amended, revoked or replaced sooner. It makes reference to this Inquiry, and notes "when completed, the conclusions from that Inquiry may give cause for the issuing Minister to review and reissue this MPS".[8]

Canada: 2017 Ministerial Directions

8. In 2017 the Canadian Minister of Public Safety and Emergence Preparedness issued Ministerial Directions on Avoiding Complicity in Mistreatment by Foreign Entities (CSIS MD), issued to

---

4 *R (on the application of Campaign Against Arms Trade) v The Secretary of State for International Trade and Intervenors* [2019] EWCA Civ 1020 20 June 2019 at [20], regarding "Criteria Guidance" on best practice in Chapter 2 of the EU "User's Guide to the European Code of Conduct on Exports of Military Equipment" (20 July 2015).

5 By letter of 10 June 2019, the NZSIS and GCSB responded to this Part in the draft report that "The agencies are bound by the law as set by Parliament and there is no legal requirement for the agencies to follow "best practice" – indeed, there would be many different interpretations of "best practice" and it would not be possible to identify which should be followed."

6 DPMC Cabinet Paper 2 *Warranting and authorisation framework* at [99] and [101].

7 Available at: https://www.nzic.govt.nz/legislation/.

8 *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities* (September 2017) (MPS Overseas Cooperation) at [67].

agencies including the Canadian Security Intelligence Services (CSIS); Royal Canadian Mounted Police (RCMP) and the Canada Border Services Agencies (CBSA). The 2017 Directions replaced the 2011 Ministerial Directions on Information-Sharing with Foreign Entities, and more clearly state the Canadian Government's "values and principles against torture and mistreatment and commitment to the rule of law", by:

- condemning torture and mistreatment;
- referring to relevant rights and protections in Canada's Charter of Rights and Freedoms;
- promising commitment to the rule of law; and
- compelling increased transparency and accountability through required reporting to review bodies, the relevant Parliamentary Committee, the Minister and the public.

9. The change in approach of Canada's 2017 MDs has been characterised as a "moral choice about the primacy given to the prohibition on torture" which, although it does not set an absolute bar in the use of torture-derived information, does represent an important shift in a contentious area where "people of utmost good faith may reasonably differ on the issue."[9]

10. The CSIS MD recognises that information-sharing with foreign entities is vital to CSIS' ability to maintain strong relationships and address threats to national security, while also recognising that torture or other CIDTP serve no legitimate military, law enforcement, or intelligence-gathering purpose, with any information yielded "very likely unreliable".[10] The CSIS MD specifically:

- Prohibits the disclosure of information, and the making of requests for information, that would result in a substantial risk of mistreatment of an individual by a foreign entity;
- Prohibits certain uses of information that was likely obtained through the mistreatment of an individual by a foreign entity;[11] and
- Provides decision-making processes for these situations.[12]

11. The CSIS MD requires CSIS to publish information that explains how the MD is implemented, including how risk assessments are conducted, in line with Canadian values including those in the Canadian Charter of Rights and Freedoms.[13] CSIS is also directed to produce a classified annual report for the Minister (and the oversight body, the Security Intelligence Review Committee (SIRC)) containing:

---

9 Craig Forcese "Touching Torture with a Ten Foot Pole" Osgoode Hall Law Journal 52.1 (2015) at 21.

10 Ministerial Direction to the Canadian Security Intelligence Service: *Avoiding Complicity in Mistreatment by Foreign Entities* (25 September 2017) (CSIS MD) at [13].

11 CSIS MD, above n 10, at [3], [13], [15] - [19].

12 CSIS MD, above n 10, at Appendices A, B and C.

13 CSIS MD, above n 10, at [19].

- details on 'substantial risk' cases where the MD was engaged, including the number of cases; and
- the restriction of any arrangements due to concerns related to mistreatment.[14]

12. Further, I note that aspects of the 2017 MDs have now been added to Bill C-59, a bill which includes significant reform of national security matters in Canada. The addition, entitled The Avoiding Complicity in Mistreatment by Foreign Entities Act, establishes a process by which written directions may be issued by the Governor in Council[15] to specific agencies, and must be issued to some agencies, including CSIS, CSE and RCMP.[16] The directions cover:

- the disclosure of information to any foreign entity that would result in a substantial risk of mistreatment[17] of an individual;
- making requests for information to any foreign entity that would result in a substantial risk of mistreatment of an individual; and
- the use of information likely to have been obtained through the mistreatment of an individual by a foreign entity.

13. With regard to accountability and transparency, the proposed Act will require immediate publication of the written directions once received and reiterates the requirement in the MD for published annual reports on the implementation of directions. While the proposed Act would not codify the substance of the MDs, it would ensure the public in Canada is aware of how information connected with torture or CIDTP is dealt with by Government agencies.[18]

14. The CSIS MD provides a useful model for the New Zealand Government to consider in the forthcoming review of the New Zealand MPSs.

Need for clarity and controls if information derived from torture is used in "exceptional circumstances"

15. UNCAT states that no exceptional circumstances or public emergency may be invoked as a justification of torture.[19] A distinction is made between committing acts of torture (which is prohibited), and using information likely obtained by torture (ie, viewed by some as permitted in "exceptional circumstances", or if received "passively"). Governments which decide to allow such use must ensure clear and strict controls exist.

---

14 CSIS MD, above n 10, at [24] and [25].

15 A process by which the Governor-General approves a decision of the Prime Minister and Cabinet.

16 On 20 June 2018, Bill C-59 was introduced to the Senate with a First Reading; The 'Avoiding Complicity' text was added in April 2018 by Canada's Standing Committee on Public Safety and National Security; The written directions are issued by the Governor-in-council to the deputy heads of the specified agencies.

17 Mistreatment is defined as torture or CIDTP as defined in UNCAT.

18 Bill C-59 received Royal Assent in June 2019.

19 UNCAT, Article 2(2).

16. The UN Special Rapporteur on torture recently stated the view that "intelligence exchanges, particularly in the context of counter-terrorism, continue to undermine the prohibition [on torture]": [20]

> "Just as is the case for judicial and administrative proceedings, the gathering and exchange of intelligence are conducted to establish the basis for potentially significant decisions by State authorities and, therefore, trigger due diligence obligations with regard to the prevention of torture and ill-treatment. … [A]ny good faith interpretation of the exclusionary rule [UNCAT, Article 15 which requires States to ensure that any statement made as a result of torture is not used as evidence in any proceeding, except against a person accused of torture] in line with its object and purpose must entail its applicability not only to judicial and administrative proceedings, but also to intelligence and executive decisions of any kind.

Define with care "exceptional circumstances" and/or "public emergency"

17. If a State considers information likely obtained by torture can be used by intelligence agencies, the exceptional circumstances or public emergency where this may occur must be clearly and appropriately defined. Such exceptional situations are colloquially described as 'ticking bomb' scenarios. The Canadian CSIS MD defines an exceptional circumstance as one where use of the information is "necessary to prevent loss of life or significant personal injury".[21] It omits the reference from the 2011 MDs to the justification of preventing "substantial damage or destruction of property".[22]

18. The House of Lords in *A and others v Secretary of State for the Home Department (No. 1)*[23] considered the nature of "a public emergency threatening the life of the nation" sufficient to derogate from the right to liberty and security in Article 5 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The Court identified that such derogations are intended to be temporary, listing the characteristics of a public emergency as:

- "it must be actual or imminent**;**
- its effects must involve the whole nation;
- the continuance of the organised life of the community must be threatened; and
- the crisis or danger must be exceptional, in that the normal measures or restrictions, permitted by the Convention for the maintenance of public safety, health and order, are plainly inadequate".[24]

19. The Dutch intelligence oversight body, the Netherlands Review Committee on the Intelligence and Security Services (CTIVD) reports that the Dutch General Intelligence and Security Service (GISS) observes the principle that information may not be shared if there are indications that

---

20 UN Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, Nils Melzer *Interim Report: Seventieth anniversary of the Universal Declaration of Human Rights: reaffirming and strengthening the prohibition of torture and other cruel, inhuman or degrading treatment or punishment* (A/73/207, July 2018) at [57].

21 CSIS MD, above n 10, at Appendix C, 1c.

22 I note this is not the approach taken in the New Zealand MPS Overseas Cooperation, above n **Error! Bookmark not defined.**8 at [28] and [46], where damage to property is included. See further section XI of the Public Inquiry Report.

23 *A and others v Secretary of State for the Home Department (No 1) (A (No 1))* [2004] UKHL 56.

24 *A (No 1)*, *a*bove n 23, at [23], citing *Greek Case (1969) 12 YB 1* at [153].

providing personal data may lead to the violation of human rights.[25] In GISS policy, this principle: [26]

> "may only be set aside *by way of rare exception.* This requires the existence of an unacceptable risk to society and its citizens that calls for prompt action. And it requires an *urgent necessity* to provide the personal data to the foreign service in question".

20. The UK Joint Committee on Human Rights described exceptional circumstances in the following terms: [27]

> "We accept that UNCAT and other provisions of human rights law do not prohibit the use of information from foreign intelligence sources, which may have been obtained under torture, to avert imminent loss of life by searches, arrests or other similar measures. We cannot accept the absolutist position on this subject advanced by some NGOs when human life, possibly many hundreds of lives, may be at stake. Indeed, where information as to an imminent attack becomes available to the UK authorities, their positive obligation to protect against loss of life under Article 2 ECHR may require them to take preventative action, even when they suspect the information may have been obtained by use of torture.
>
> However great care must be taken to ensure that use of such information is only made in cases of imminent threat to life. Care must also be taken to ensure that the use of information in this way, and in particular any regular or repeated use of such information, especially from the same source or sources, does not render the UK authorities complicit in torture by lending tacit support or agreement to the use of torture or inhuman treatment as a means of obtaining information which might be useful to the UK in preventing terrorist attacks. Ways need to be found to reduce and, we would hope, eliminate dependence on such information".

21. Lastly, it is useful to note that the 'ticking bomb' scenarios assume: [28]

> "that you always have the right suspect in custody, the bomb is always real, the suspect always has the information you need, the suspect always talks when tortured, and the information the suspect then provides is always sufficiently accurate and detailed to avert the looming catastrophe".

22. As Brecher points out in *Torture and the Ticking Bomb,* "in the real world none of these variables is quite so assured".[29]

Place explicit limits on permissible use of torture-derived information in emergencies

23. Canada's CSIS MD for sets out the following limits:

- Information likely obtained through mistreatment may not be used:
  - in a way that creates a substantial risk of further mistreatment;
  - as evidence in any judicial, administrative or other proceedings; or

---

25 CTIVD *Review Report 22a on the cooperation by GISS with foreign intelligence and security services* (2009) at 24.

26 CTIVD *Review Report 22a*, above n 25, at 24 (emphasis as per original).

27 UK JCHR *The UN Convention Against Torture* (Session 2005-6 HL Paper 185-1, HC 701-1) at [55].

28 Richard Barrett and Tom Parker "Acting ethically in the shadows: Intelligence gathering and human rights" 236 to 264, at 250; in Manfred Nowak and Anne Charbord (eds) *Using Human Rights to Counter Terrorism* (Edward Elgar Publishing, United Kingdom, 2018).

29 Bob Brecher *Torture and the Ticking Bomb* (Blackwell Publishing, Oxford, 2007).

- to deprive someone of their rights or freedoms, except where the Director of CSIS or senior official designated by the Director authorises such use because it is necessary to prevent loss of life or significant personal injury;

- Where such exceptional circumstances exist, "[t]he information must be accurately described, and its reliability properly characterized using caveats making clear that the use of this information has been authorized for a clearly defined and limited purpose";

- The Minister, the oversight body SIRC, and the relevant Parliamentary Committees must be informed as soon as feasible and provided with the relevant contextual information.[30]

24. The *Ottawa Principles on Anti-terrorism and Human Rights,* formulated in 2006 by Canadian civil society and academics, recommend similar but more broadly-framed limits to maintain and respect the non-derogable nature of UNCAT:[31]

> "Information, data or intelligence that has been obtained through torture or cruel, inhuman or degrading treatment or punishment may not be used as a basis for:
>
> - the deprivation of liberty;
> - the transfer, through any means, of an individual from the custody of one State to another;
> - the designation of an individual as a person of interest, a security threat or a terrorist or by any other description purporting to link that individual to terrorist activities; or
> - the deprivation of any other internationally protected human right."

Ensure realistic assessments of the reliability and credibility of torture-derived information

25. The CSIS MD states that torture and CIDPT serve no legitimate intelligence-gathering purpose with any information yielded "very likely unreliable".[32]

26. Further, the use of such information by government may potentially affect public perceptions around the integrity and credibility of executive decision-making. Courts in relevant jurisdictions have noted the negative effect admitting evidence obtained by torture would have on perceptions of the integrity of the courts and systems of justice.[33] But to date the same attention and analysis has not been applied to the use of torture-derived information in executive and operational decision-making.

27. The Report of the Association for the Prevention of Torture summarises those wider effects as follows:

- Using the spoils of torture encourages it, and gives torture an ill-defined credibility;

---

30 CSIS MD, above n 10, at Appendix C.

31 University of Ottawa Faculty of Law *Principles on Anti-terrorism and Human Rights* (2006) Principle 4.3.2.

32 CSIS MD, above n 10, at [13].

33 See, for example, *A and others v Secretary of State for the Home Department (No 2)* [2005] UKHL 71; [2006] 2 AC 221; [2006] 1 All ER 575 (*A (No 2)*), at [52].

- Torture-tainted information is inherently unreliable;[34]
- Relying on tainted information wastes resource;
- It raises questions around the propriety of agency action, given torture is immoral and unethical.[35]

28. Applying this, if a New Zealand Minister were to direct that torture-derived information could be used by intelligence and security agencies in exceptional circumstances, at a minimum that information should, on a best practice approach, be accurately labelled; its reliability properly characterised; employing caveats to make clear that its use is authorised for the clearly defined and constrained purpose; with retention periods identified and followed by a presumption of destruction.

29. An evaluative committee on information sharing in the Canadian context[36] considers relevant contextual aspects drawn from Canadian case law[37] and UN Committee interpretations.[38] These practical aspects are instructive and can contribute to any assessment of the reliability of information received:

- Persons most targeted by torture are political detainees and perceived terrorists;
- The more self-inculpatory the nature of the information provided by an individual, the less likely it was provided voluntarily;
- Corroborated intelligence does not mean that it has not been derived from torture; the level of detail or the reliability of the information are not, on their own, useful factors in assessing whether there are reasonable grounds to believe that information was obtained by torture; the issue is not whether it is true or false, or corroborated or not but whether it is obtained by torture;
- It is widely accepted that reports from Amnesty International, Human Rights Watch and the UN Committee Against Torture represent the best evidence available since there is very little direct evidence of torture;
- CSIS cannot simply rely upon anecdotal information or personal relationships that may exist between special liaison officers and security officials in foreign countries (as those with poor human rights records may be more interested in maintaining a relationship with the Service than actually providing truthful information on human rights conditions);

---

34 See further references on the reliability of information obtained by torture in Part D3 and Part F4.1.

35 Association for the Prevention of Torture *Beware the gift of poison fruit: Sharing information with States that torture* (2012) at 17 and 18. See also Sarah Fulton "Cooperating with the enemy of mankind: Can States simply turn a blind eye to torture" (2012) 16(5) International Journal of Human Rights at 773 - 795.

36 As discussed further below.

37 *In relation to Mahjoub's Security Certificate* (2010) FC 787 at [196] - [204] and [206] - [207] per Blanchard J.

38 Referenced to UNCAT.

- To establish that information was obtained by the use of torture requires more than simply pointing to the poor human rights records of a given country.

Define the applicable law in a guide

30. Prudent practice is to provide a standalone guide to the applicable law, both domestic and international, to inform staff (including if in-theatre) and which can then be referenced by other related policies and procedures. Setting out the legal standards can act as a quick reference to existing benchmarks, which will be relevant if, for example, another State appears to be relying on a different interpretation of the law or signals that it has or will cease to apply relevant legal obligations.

31. The UN Special Rapporteur's *Compilation of good practices* assumes that intelligence services have this understanding of the applicable law firmly in place. For example, Practice 35 recommends that: [39]

> "Intelligence services are explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities. If States request foreign intelligence services to undertake activities on their behalf, they require these services to comply with the same legal standards that would apply if the activities were undertaken by their own intelligence services."

Create agreements between States/agencies outlining provision of assistance and information sharing

32. We acknowledge that there are overarching and more formal arrangements already in place, some long-standing, some as written agreements, between the GCSB or the NZSIS and their foreign intelligence partners. These high-level arrangements[40] deal with information sharing and the necessity for the partner agencies to comply not only with their own domestic law and policies but also that of their partners. However, access to the terms of these arrangements has not proved possible so we are unable to assess whether they adequately address best practice including human rights compliance. What is set out below should be read in that light. We also suggest that the NZSIS and GCSB review information sharing agreements, where they do or should exist, with these elements in mind.

33. To address the requirements for transparency and accountability of actions, best practice for information sharing arrangements between States (or between their agencies) directs that such agreements or MOUs must:

    - be in writing;
    - be signed off by Directors and/or Ministers;
    - set out rules (ie mutually agreed standards and expectations) governing the use of shared information, not least to "reduce the scope for informal

---

39 UN Special Rapporteur 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* A/HRC/14/46 (2010) at [49].

40 These are separate from specific Ministerial Authorisations under ISA (eg, under s 10(1)(b)(iii)). See Cullen and Reddy, above n 2, at [3.44] and [3.47].

intelligence-sharing which cannot be easily reviewed by oversight institutions";[41]

- include a statement of parties' compliance with human rights and data protection requirements;
- include a requirement to observe in practice the 'third party rule' or where more appropriate, the 'third country rule' (ie where information obtained may only be provided to others if the service/country from which the information originates has given permission to do so);[42]
- address the situation where the NZSIS or GCSB receives information at third hand (ie where the information is disclosed to New Zealand by a liaison service not suspected of mistreatment of individuals but which obtained that information indirectly from a third party which is);[43]
- make provision for the sending service to request feedback on the use of the shared information;[44]
- be regularly reviewed;[45]
- when concluded or revised, be provided to independent oversight institutions for review.[46]

34. Canada provides an example of oversight of such arrangements. As with the New Zealand intelligence and security agencies,[47] CSIS is required by statute to have Ministerial approval for information sharing arrangements with foreign intelligence agencies.[48] CSIS is also required by statute[49] to provide the oversight body, SIRC, with a copy of any written arrangement that CSIS enters into with the government of a foreign State; any institution therein; or any international organisation of States or an institution of such a body.[50] SIRC must "carefully examine these arrangements and monitor the exchange of information to ensure that the terms of the arrangements are upheld".[51]

---

41 Martin Scheinin *Compilation of good practices*, above n 39, at [45].
42 CTIVD *Review Report 22a*, above n 25, at 22 and 23.
43 UK Intelligence Services Commissioner Rt Hon Sir Mark Waller *Supplementary to the Annual Report for 2015* (House of Commons, HC 458, 2016) identifying this as a gap in the *Consolidated Guidance*.
44 Martin Scheinin *Compilation of good practices,* above n 39, at [45].
45 Canada Commission of Inquiry *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Canada Privy Council) Ottawa: Public Works and Government Services Canada, Volume 3, 2006 at 321.
46 Privacy International Report *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards* April 2018, at 44, 47 to 48; Martin Scheinin *Compilation of good practices,* above n 39, at [48] - [49].
47 Intelligence and Security Act 2017 (ISA) ss 10 and 12.
48 Canada Security and Intelligence Service Act 2002, ss 13 and 16.
49 Canada Security and Intelligence Service Act, s 17.
50 Privacy International Report *Secret Global Surveillance Networks,* above n 46, at 34.
51 CSIS 'Sharing Intelligence Internationally', accessed at https://csis.gc.ca//bts//shrng-en.php.

Have a policy to guide informed assessments of State/agency human rights records and accurately identify risks around engagement

35. To properly manage uncertainty and legal risk around engaging with the activities of foreign intelligence and security agencies, including any potential differences in approach to international legal obligations, information sharing and cooperation must proceed on a fully informed basis. The UN Special Rapporteur, recommended that, before either entering into an intelligence-sharing agreement or sharing intelligence on an *ad hoc* basis, intelligence services undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart (and whether there is independent oversight). Before handing over information, intelligence services should make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and will not be used for purposes that violate human rights.[52]

36. Sections 3, 17 and 18 of the ISA require the GCSB and the NZSIS to act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law. Implicit in those obligations is a need to be actively thinking, asking questions and assessing where and how risks of being implicated in acts of torture or CIDTP by other States and agencies with whom they engage or with whom they are establishing relationships might arise.[53]

Policy to establish an appropriate overall framework and process

37. Policies in partner jurisdictions outline the scheme of inquiry to be followed. The UK *Consolidated Guidance* applies in particular to the detention and interviewing of detainees overseas, and the passing and receipt of intelligence relating to detainees. It states that when working with foreign authorities:

- UK agency personnel must follow the letter and the spirit of the *Guidance*, which accords with the UK's own international and domestic legal obligations;
- great care must be taken to assess whether there is a real risk that a detainee will be subjected to: unlawful killing; torture; CIDT; extraordinary rendition or rendition; or unacceptable standards of arrest and detention;
- the UK will investigate whether it is possible to mitigate any such risk;
- When, despite efforts to mitigate the risk, there are grounds to believe there is a real risk of torture, unlawful killing or rendition, the presumption is that the UK agencies will not proceed.[54]

---

52 Martin Scheinin *Compilation of good practices,* above n 39, at [47].

53 As reflected in the MPS Overseas Cooperation (2017), above n 8 which refers to "a duty to apply due diligence" at [36].

54 UK Government *The Principles relating to the detention and interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees* (referred to as the *Consolidated Guidance)* (July 2019) at [2] and [3]. The *Consolidated Guidance* requires each agency to whom these Principles apply to provide more detailed advice and guidance (including legal) to their personnel (at page 1).

38. *Human Rights Guidance*, by the UK's Overseas Security and Justice Assistance (OSJA), addresses a wider range of activities overseas than the *Consolidated Guidance* (and the *Guidance* directs UK personnel to also consider OSJA). It sets out a four-step inquiry, called AIMS:

- **Assess** the internal situation in the host country (eg, stability, practice towards human rights and IHL);
- **Identify** the human rights, IHL, political and reputational risks associated with the proposed assistance;
- **Mitigate** the identified risks, if possible (including considering when/how to stop providing assistance if there is a significant change); and
- **Strengthen** compliance with human rights and IHL in the host country through the assistance (ie, make an overall assessment of whether there is a *serious risk* that the assistance might *directly or significantly contribute* to a violation of human rights, IHL or lead to political or reputational risk).[55]

39. The provision of comprehensive templates and checklists can inform and greatly assist staff in making these sometimes complex assessments, and ensure appropriate sign-off for any further action taken.

Policy to inform assessment of State/agency human rights records

40. The Netherland's CTIVD, noting the difficulty in the GISS finding out whether information from a foreign agency has been obtained by torture, stated that: [56]

> "This makes it all the more important that the GISS, before and while it cooperates with a foreign intelligence or security service, assesses carefully to what extent the human rights situation in a country constitutes an obstacle to cooperation with the relevant service of that country."

41. An assessment of the current level of risk of human rights breaches by the State itself is an indicative starting point, before scrutinising specific State agencies.[57] For some country assessments, it may be appropriate to require cross-government input, for example, from the Ministry of Foreign Affairs and Trade, perhaps accommodated through ODESC.

42. Policy guidance for making these assessments must include the range of credible sources for officials to consult. There are many reliable and accessible sources that provide information about a State's human rights record, including (in no specific order):

- discussions with State authorities (including at diplomatic and ministerial levels);

---

55 UK Government *Overseas Security and Justice Assistance Human Rights Guidance* (2017) at [21] (emphasis as per original).

56 CTIVD *Review Report 22a*, above n 25, at [14.2].

57 CTIVD *Review Report 22a,* above n 25, at [24]; "Merely the country to which the foreign service concerned belongs may already constitute an indication."

- Governmental reports and published Government legal opinions;[58]
- Ministerial directives;
- reports of Parliamentary committees;[59]
- Presidential orders;[60]
- public statements and official policies of the foreign agency or State;[61]
- reports of fact-finding commissions and independent monitors;
- reports from States' independent oversight agencies (eg oversight of human rights or intelligence and security matters);
- country profiles drawn up by the Ministry of Foreign Affairs and Trade, and reports from embassies;
- UN reports (eg, country visits by Special Rapporteurs; Concluding Observations by the Committee Against Torture, on State compliance with UNCAT; Concluding Observations by the UN Human Rights Committee, on State compliance with ICCPR; Reports from UN Assistance Mission in Afghanistan (UNAMA));
- Council of Europe reports;
- US State Department country reports;
- International Committee of Red Cross (ICRC) reports;
- relevant caselaw (eg, European Court of Human Rights; UK, Canadian and NZ Supreme Courts);
- recent reports from civil society and independent international human rights protection organisations (eg NGOs such as Amnesty International and Human Rights Watch);[62]
- information from partner agencies and other States; and

---

58 For example, Office of Legal Counsel in US Department of Justice; selected opinions are published on DoJ's website.

59 For example, the UK Parliament's Joint Committee on Human Rights.

60 A recent example is US President Trump's Executive Order 13823 of 30 January 2018 *Protecting America Through Lawful Detention of Terrorists* in which it is ordered at 1.(d) that "[t]he detention operations at the U.S. Naval Station Guantanamo Bay are legal, safe, humane, and conducted consistent with United States and International law".

61 See Erika de Wet "Complicity in the Violations of Human Rights and Humanitarian Law by Incumbent Governments through Direct Military Assistance on Request" (2018) 67 ICLQ at 18, citing V Lanovoy *Complicity and its Limits in the Law of International Responsibility* (Hart Publishing, Oxford, 2016) at 101 and 238.

62 When considering potential breaches of IHL by a trading partner, Saudi Arabia, the UK Foreign Office reported in October 2015 that "we have taken into account recent NGO reports in our assessment and we are ensuring that we are meeting our responsibility to avoid any risk of "wilful blindness"; as referenced by the High Court in *Campaign Against the Arms Trade v Secretary of State for International Trade* [2017] EWHC 1754 (Admin) at [154].

- media reports.

43. In addition, knowledge of wrongful conduct and its duration may be gained through long-standing prior cooperation with a foreign agency, or from geographical proximity.

44. In short, to ensure a current and reliable assessment of a country's human rights record, there is no one source of truth. To adequately reflect this, the relevant policy must provide comprehensive guidance as to useful sources (eg with links on an online appendix). What is required is:[63]

> "… a classic 'risk assessment'. This involves looking at all the information in the round, of which the recipient's 'past and present record' is part. Past and present conduct is one indicator as to future behaviour ..."

Policy to require assessments that include the treatment of detainees

45. To assess the treatment of detained individuals, the policy must guide officials to consult reports on conditions in a State's detention facilities, for example, reports from a National Preventive Mechanism established under the Optional Protocol to UNCAT. The UK Government's *Consolidated Guidance*[64] requires an assessment of whether there is real risk of torture, before, for example:

- Passing intelligence to a foreign authority concerning an individual detained by that authority or likely to be detained by that authority as a result of that intelligence; and

- Receiving unsolicited intelligence that has been obtained from a detainee in the custody of a foreign authority.

46. When CSIS is considering using information received from or sent to a foreign entity, risk assessment criteria include asking questions about the detention status of the individual, plus whether the information comes from a self-incriminating confession and if there is other information indicating potential mistreatment, such as a poor human rights record or a practice of extraordinary rendition.[65]

---

63 *Campaign Against the Arms Trade v Secretary of State for International Trade,* above n 62*,* at [181.iii]. This view was reiterated by the Court of Appeal "[T]he User's Guide calls specific attention to the question of past violation as a relevant consideration when assessing whether there is a real risk of future violation. In our view that is obviously correct. How could it reasonably be otherwise?" The Court of Appeal held that the Secretary of State had erred in law by making no assessment of whether Saudi Arabia (leading the Coalition in the Yemen conflict) had committed past violations of IHL, and so whether there was a "real risk" for the future, and whether Saudi Arabia had "genuine intent" and "capacity to live up to the commitments made". The Court's decision resulted in the UK International Trade Secretary having to review past decisions on arms sales to Saudi Arabia and temporarily suspend any new ones. *R (on the application of Campaign Against Arms Trade) v The Secretary of State for International Trade and Intervenors* [2019] EWCA Civ 1020 20 June 2019 at [138] to [144].

64 UK *Consolidated Guidance*, above n 54, at [6].

65 Canadian Security Intelligence Service, Deputy Director Operations' Directive *Information sharing with foreign entities* (issued under the 2011 Ministerial Direction; released under the Access to Information Act).

Policy to provide links to sources – Library of previous country assessments

47. Both a policy with links to the sources as listed above, and a library of the agency's previous country assessments, provide sound reference points for operational staff. For example, after some seven years of recommendations to establish such a point of reference, the UK Cabinet Office in 2017 told the Intelligence and Security Committee that it was establishing a team in early 2018: [66]

> "to create a central SIA [Security and Intelligence Agencies] reference point collating risk assessments, submissions, assurances, mistreatment reporting, OSJAs, and open source assessments, to ensure that SIA risk assessments are made on a consistent basis, or at least with a consistent reference base".

Ask the hard questions to inform assessments

48. A key element of best practice is an agency's willingness to ask the difficult but essential questions, to assess the level of risk involved in engaging with activities of a foreign agency. This is particularly the case when specific indications of human rights breaches necessitate questions to an agency with which there is a long-standing relationship. Various jurisdictions have considered this broad question, in different contexts and provide useful guidance. In *Chahal v United Kingdom*[67] the ECHR identified the need for States to make a "rigorous examination" and exercise "close scrutiny" with regard to potential evidence of torture.[68] The recent report of the UK House of Lords Select Committee on International Relations, "Yemen: giving peace a chance", regarding the sale of arms to Saudi Arabia in light of the war in Yemen, stated that "Relying on assurances by Saudi Arabia and Saudi-led review processes is not an adequate way of implementing the obligations for a risk-based assessment set out in the Arms Trade Treaty".[69]

49. The ECHR has held that "the existence of the alleged risk must be assessed primarily with reference to those facts which were known or ought to have been known" to the State at the time".[70] For focused inquiries around a State's human rights practices, the Council of the European Union *User's Guide* on the export of military equipment is instructive. Initial questions can include whether there are "consistent reports of concern from local or international NGOs and the media". Further, inquiries are made about indicators of human rights practices, such as:

    - The degree of cooperation with international and regional human rights mechanisms (eg, UN treaty bodies and special procedures); and

---

66 UK ISC *Detainee Mistreatment and Renditions: Current Issues* (HL 1114, 28 June 2018)(UK ISC *Current Issues*) at [129].

67 *Chahal v United Kingdom* (1996) 23 EHRR 413.

68 For accepted standards of investigation into acts of torture in a State's territory, see the UN *Manual on the Effective Investigation and Documentation of Torture and Other Cruel Inhuman or Degrading Treatment or Punishment* (The Istanbul Protocol), Professional Training Series (No 8/Rev 1) 2004; The fundamental principles of any viable investigation into alleged incidents of torture are competence, impartiality, independence, promptness and thoroughness.

69 UK House of Lords Select Committee on International Relations, *6th Report of Session 2017 – 19* (16 February 2019) at [72].

70 *Abu Zubaydah v Lithuania* (application no 46454/11) ECHR 31 May 2018, at [585].

- The political will to discuss domestic human rights issues in a transparent manner, for instance in the form of bilateral or multilateral dialogues, with the EU or other partners including civil society.[71]

50. A decision-maker should be able to satisfactorily explain why it was not considered necessary to have regard to credibly-sourced reports of State or agency involvement in acts of torture, and adjust the intelligence exchanges or cooperation accordingly, if that was the case.

51. An appropriate level of government inquiry into a risk of torture and ill-treatment was addressed in the June 2006 Report by the Council of Europe Committee on Legal Affairs and Human Rights. The Report addressed the abuse of detainees through extraordinary rendition and secret detention sites run by the CIA in Europe, and held authorities in the relevant States: [72]

> "… responsible for failing to comply with the positive obligation to diligently investigate any serious allegation of fundamental human rights violations".

52. That Report, in a chapter "Attitude of governments", stated that: [73]

> "[I]t has to be said that most governments did not seem particularly eager to establish the alleged facts. The body of information gathered makes it unlikely that European States were completely unaware of what, in the context of the fight against international terrorism, was happening at some of their airports, in their airspace or at American bases located on their territory. Insofar as they did not know, they did not want to know. It is inconceivable that certain operations conducted by American services could have taken place without the active participation, or at least the collusion, of national intelligence services. If this were the case, one would be justified in seriously questioning the effectiveness, and therefore the legitimacy, of such services. The main concern of some governments was clearly to avoid disturbing their relationships with the United States, a crucial partner and ally. Other governments apparently work on the assumption that any information learned via their intelligence services is not supposed to be known".

53. In 2007 the European Parliament passed a Resolution that "Deplores the fact that the governments of European countries did not feel the need to ask the US Government for clarifications regarding the existence of secret prisons outside US territory".[74]

Require assessment of all unsolicited information received by agencies

54. In the context of information sharing relationships between States, information that is received unsolicited by intelligence and security agencies must nevertheless be subject to

---

71 Council of the European Union *User's Guide to Council Common Position* 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment, see *Section 2: Best practice for the interpretation of Criterion Two* at 38 to 54, and factors relevant to serious human rights violations at 40 to 41; UK High Court and Court of Appeal referenced the *User's Guide* in *Campaign Against Arms Trade,* above n 62 and n 63.

72 Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights, Report of investigation into CIA secret detention sites by Senator Dick Marty (7 June 2006) at [287]; cited in *Abu Zubaydah v Lithuania*, above n 70, at [273].

73 Parliamentary Assembly of the Council of Europe, Report of investigation into CIA secret detention sites, above n 72, at [230]; cited in *Abu Zubaydah v Lithuania,* above n 70 at [272].

74 European Parliament *Resolution on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners* (2006/22009INI, 14 February 2007) at [9]; cited in *Abu Zubaydah v Lithuania,* above n 70, at [286].

comparable legal constraints, inquiry, analysis and rigour as all other information sought or sent.

55. The UK *Consolidated Guidance*, which defines 'unsolicited' as intelligence not requested or otherwise sought, including intelligence received as part of general intelligence sharing, states that: [75]

> "where personnel receive unsolicited intelligence from a foreign authority that they know or believe has originated from a detainee, and there is a real risk the detainee has been or will be subject to relevant conduct, senior personnel must be informed. In all cases where the senior personnel believe the concerns to be valid, Ministers must be notified of the concerns. …
>
> In such instances, the relevant authorities will consider whether action is required to avoid the foreign authority believing that HMG's continued receipt of intelligence is an encouragement of the methods used to obtain it or adversely affects the conditions under which the detainee is held. Such action could, for example, include obtaining assurances, or demarches on intelligence and/or diplomatic channels. They will also consider whether the concerns were such that this would have an impact on engagement with that foreign authority in relation to other detainees".

Mitigate risks of torture or cruel, inhuman or degrading treatment or punishment

56. States have a range of measures at their disposal which, depending on the circumstances, may serve to mitigate the risk that their actions are associated with torture or cruel, inhuman or degrading treatment or punishment. Reliance on one measure alone will seldom provide sufficient mitigation or reduction of risk. Nor will a substantial reliance on caveats and assurances without accompanying comprehensive assessments and monitoring of the human rights record and practices of the country/agency. On the other hand, mitigation of risk may be achieved simply by editing the information to omit identifying information of individuals.[76]

57. Another approach when real risk exists is to make assistance conditional. Although not in the context of intelligence sharing the 2015 UNAMA report on the treatment of detainees in Afghanistan recommended that Donor States and those contributing troops should:[77]

> "Ensure that torture and ill–treatment of detainees by the National Directorate of Security, Ministry of Interior/Afghanistan National Police and Afghanistan National Army and implementation of effective remedial measures including legal obligations to hold perpetrators of torture accountable, are considered as key progress and conditionality indicators in making determinations on … overall provision of technical support, advice, assistance and training to implicated Afghan institutions and ministries."

58. The main tools used by intelligence and security agencies to mitigate identified risk are caveats, assurances and legal initiatives.

---

75 UK *Consolidated Guidance* (2019) above n 54, at [11] and [12].

76 Canada Communications Security Establishment, Operational Policy OPS-6, *Policy on Mistreatment Risk Management* (2 August 2016) at [3.6].

77 UN Office of High Commissioner for Human Rights and UN Assistance Mission in Afghanistan *Update on the Treatment of Conflict-Related Detainees in Afghan Custody: Accountability and Implementation of Presidential Decree 129* February 2015, Kabul, Afghanistan at 113 and 114.

Mitigation tool: Caveats

59. The caveat system is widely used and based on trust. In essence it describes directions on permissible use, attached to information when dispatched. Caveats do not guarantee that a recipient of information to which a caveat is attached will honour that caveat. The system is primarily about source protection. Caveats are not legally enforceable.[78] However, the ability and willingness of agencies to respect caveats and seek consent before using information will affect the willingness of others to provide information in the future – a significant incentive for agencies to respect caveats. "Common sense tells us the incentive is greater when caveats are clear and in writing."[79]

60. The Arar Commission Report included the following recommendations, which emphasise the limitations of lawful reliance on caveats: [80]

> "Never share information in a national security investigation without attaching written caveats in accordance with an existing policy stating:
> - which institutions are entitled to have access to the information subject to the caveat;
> - what use the institution may make of that information; and
> - a clear process (and contact person) for recipients to follow to seek changes to the permitted distribution and use of the information".

61. The Arar Report states that implied caveats (ie, unwritten understandings) are not an adequate substitute. It further identifies issues with the ability of a State to control out-bound information once conveyed to a foreign agency. The attachment of caveats, such as originator control and limits on use, are obviously "effective only where foreign agencies choose to abide by them", with accompanying difficulties of detecting tacit information sharing done in violation.[81] Therefore, agencies should as far as practicable establish procedures to monitor adherence to caveats when sharing information, and consider reporting breaches to independent oversight bodies.[82]

Mitigation tool: Assurances

62. Diplomatic assurances take a variety of forms, ranging from oral to written documents signed by officials from both governments. Assurances may restate commitment to the state's international law obligations or more specifically address what it will do or not do in a particular situation, such as intelligence sharing or deportation.[83] There is no general rule or practice at international law preventing a state from seeking and obtaining assurances where

---

78 UK ISC *Detainee Mistreatment and Rendition: Current Issues*, above n 66, at [143].

79 Canada Commission of Inquiry *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, above n 45, at 106 and 107.

80 Canada Commission of Inquiry *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, above n 45, at Recommendation 9.

81 Craig Forcese "Touching Torture with a Ten-Foot Pole" Osgoode Hall Law Journal, 52.1 (2015) at 270.

82 Privacy International Report *Secret Global Surveillance Networks,* above n 46, at 45.

83 In a paper on "International Legal Issues Relating to Detention", presented to the Government Inquiry into Operation Burnham, on 30 July 2019, Dr Penny Ridings noted safeguards to assist compliance with non-refoulement obligations relating to deportation, including assurances: "Additional safeguards that assist with complying with the non-refoulement obligation are the obtaining of formal assurances that a detainee will be treated in accordance with international human rights standards. Assurances are usually considered in combination with complementary mechanisms, such as monitoring of detainees, … efforts to gather and maintain knowledge about law enforcement and detention facilities".

a risk of torture is at issue, although such assurances are not legally enforceable and will not absolve a state of its duty to comply with its international law obligations.

63. Assurances must be practical and meaningful, with regard to the actions a State will take on receiving the information in question, or upon receiving the transferred/deported individual. Obvious considerations relate to whether an individual to be deported or identified in the information will be detained and the State's record of treatment of detainees. Mere assurances that the activities of foreign agents will comply with international and national law, although frequently seen, may not be considered sufficient to ensure adequate protection against the risk of torture or ill treatment.

64. Assurances have, in some circumstances, proved unreliable. With regard to the CIA's extraordinary rendition of detainees from CIA-run 'black sites' in European States, it was submitted to the ECHR that by 2005: [84]

> "any Contracting Party would or should have known that any US assurances that a detainee previously subjected to the US programme would be treated in a manner consistent with international law, in the case of further transfer, lacked credibility".

65. The House of Lords in *RB and U (Algeria) and OO (Jordan) v Secretary of State for the Home Department*[85] held that such assurances need to provide a reliable guarantee; the absence or otherwise of torture or ill-treatment in a country is a question of fact; and, should reliable sources point to a real risk of torture or ill-treatment in that country, it will not matter what assurances have been given. Further, UN experts have observed that:

> "[i]t is therefore unclear why States that violate obligations under treaty and customary international law should comply with non-binding assurances".[86]

66. The Afghanistan Government's Ministry of Foreign Affairs in 2009 provided an assurance to the NZDF, set out in an "Arrangement" for "the transfer of persons between the New Zealand Defence Force and the Afghan Authorities" with regard to observing human rights obligations for the treatment of detainees. The Arrangement states *inter alia* that both participants will "observe applicable international and domestic law".[87] While further detail on the applicable legal obligations would have been preferable, I note this Arrangement was not the only mechanism NZDF relied upon to monitor the treatment of any detainees.

67. The subsequent decision of the High Court of England and Wales in *R (on application of Maya Evans) v Secretary of State for Defence*[88] considered the nature and effectiveness of formal assurances made to the UK forces by the Afghanistan Government, to similarly observe human rights in the treatment of transferred detainees. The Court concluded that, despite genuine

---

84 *Abu Zubaydah v Lithuania*, above n 70, at [471]; submissions by the International Commission of Jurists and Amnesty International.

85 *RB and U (Algeria) and OO (Jordan) v Secretary of State for the Home Department* [2009] UKHL 1.

86 Statement by UN Special Rapporteur on torture, Juan Mendez and Special Rapporteur on Human Rights and Counter-Terrorism, Ben Emmerson "UN rights experts concerned about fate of Guantanamo detainee deported to Algeria" *UN News* (10 December 2013).

87 *Arrangement Between the Ministry of Foreign Affairs of the Islamic Republic of Afghanistan and the New Zealand Defence Force Concerning the Transfer of Persons Between the New Zealand Defence Force and the Afghan Authorities* 12 August 2009.

88 *R (on application of Maya Evans) v Secretary of State for Defence* [2010] EWHC 1445 (Admin).

efforts by UK forces to ensure the arrangements were accepted by relevant Afghanistan authorities, reliance on such assurances was misplaced given the public record of mistreatment of detainees by several Afghanistan authorities.[89] Instead, the critical question was how those arrangements operated in practice.

68. The comprehensive 2017 UK report *Deportation with assurances* by David Anderson QC and Professor Clive Walker QC observed, "deportation with assurances is not at all realistic for chronically 'problematic' countries or 'countries of concern'".[90] That report concludes:[91]

> "The key consideration to be taken into account in developing safety on return processes is whether compliance with assurances can be objectively verified through diplomatic or other monitoring mechanisms".

69. The UN Committee Against Torture has also expressed concern about State party reliance on assurances or other kinds of guarantees, assumptions that a person will not be tortured if transferred to another State, the secrecy of such procedures including the absence of judicial scrutiny, and lack of monitoring mechanisms put in place to assess if the assurances have been honoured.[92] Further, monitoring regimes associated with assurances cannot prevent torture, they can only detect acts of torture after they occur.[93]

70. Experience demonstrates that assurances should be established in writing. But the 2018 UK ISC Report on *Detainee Mistreatment and Rendition: Current Issues* identified that obtaining assurances in writing can be problematic, as "it can be taken to imply suspicion", "undermine trust and jeopardise future cooperation".[94] The Committee recommended that: [95]

> "where it is not possible to obtain a written assurance from a liaison partner, a written record of the oral assurance should be produced and sent to the liaison partner so that there is a shared understanding of expectations".

<u>The New Zealand position on assurances</u>

71. The New Zealand Government's official stance on assurances, to mitigate an identified risk of torture or other mistreatment, was articulated to the Committee Against Torture in March 2017.[96] New Zealand's position was that, while it shared the Committee's view that diplomatic assurances should not be used to undermine the principle of non-refoulement, the practice

---

89 *R (on application of Maya Evans),* above n 88.

90 David Anderson QC and Professor Clive Walker QC *Deportation with assurances* ((House of Commons, CM 9462, July 2017) at [7.6].

91 Anderson and Walker *Deportation with assurances*, above n 90, at [3.36] - [3.42].

92 Committee Against Torture *Concluding Observations Periodic Report of United States of America* CAT/C/USA/CO/2 (25 July 2006) at [21]; See also Committee Against Torture *Concluding Observations Periodic Report of United States of America* CAT/C/USA/CO/3-5 (19 December 2014) at [16]; *Agiza v Sweden Committee Against Torture* CAT/C/34/D/233/2003 (20 May 2003) at [13.4].

93 Omar Sabry *Torture of Afghan Detainees* (Canadian Centre for Policy Alternatives, 2015).

94 UK ISC *Current Issues*, above n 66, at [62] Recommendation V.

95 UK ISC *Current Issues,* above n 66, at [62] Recommendation V.

96 New Zealand Government "Observations of New Zealand on the Committee Against Torture's draft revised General Comment No.1 (2017) on the Implementation of Article 3 of the Convention on the Context of Article 22" (24 March 2017); Responding to the Committee's *Draft General Comment No 1 (2017) on the implementation of Article 3 of the Convention in the context of Article 22*, Committee Against Torture 60th session CAT/C/60/R.2 (2 February 2017); Now confirmed as *General Comment No. 4 (2017) on the implementation of article 3 of the Convention in the context of article 22* (Advance unedited version, 9 February 2018).

of such assurances is well-established internationally and there can be circumstances in which assurances meet certain minimum quality and reliability thresholds, so it is possible for a State to take diplomatic assurances into account consistent with the principle of non-refoulement. It will depend on all the factors of a case, including the human rights situation in the receiving State, the risk factors associated with the individual, and the quality and practical enforceability of the assurances.

72. Recently the New Zealand Court of Appeal reviewed a decision by the (former) Minister of Justice to allow the extradition of a Mr Kim to the People's Republic of China (PRC).[97] The High Court had held that the Minister of Justice was entitled in principle to rely on the nature and quality of Chinese Government's assurances.[98] The Court of Appeal quashed the decision, with the current Minister of Justice to reconsider whether Mr Kim is to be surrendered. The Court of Appeal confirmed that New Zealand is not prohibited from accepting or relying on diplomatic assurances when assessing whether there is a substantial risk that a person will be tortured or otherwise subjected to breaches of human rights.[99] However, the Court held that consideration of the preliminary question, whether the general human rights situation in China is such that assurances should not be sought or accepted, was not sufficient.[100] Further, relevant evidence asserting that murder-accused were at high-risk of torture could not reasonably be put to one side.[101] The Court held that the Minister erred in failing to address inadequacies in the assurances and how they could protect against torture in China when:[102]

- Torture is already against the law, yet persists;
- The practice of torture is concealed by the State and its use can be difficult to detect;
- Torture often occurs outside the videotaped interrogation;
- Evidence obtained by torture is frequently admitted in court; and
- There are substantial disincentives for anyone, including the detained person, reporting the practice of torture.

<u>Practical factors for considering assurances</u>

73. Practical factors to take into account, in evaluating the appropriate use of assurances and whether received assurances can be relied upon, are broadly instructive and applicable across a number of areas, such as information sharing. These factors include:

For assurances developed with regard to deportation:

- a preliminary question of whether the general human rights situation in the receiving State excludes accepting any assurances whatsoever (eg, including

97 *Kyung Yup Kim v Minister of Justice and the Attorney-General* [2019] NZCA 2019, 11 June 2019.

98 *Kyung Yup Kim v Minister of Justice and the Attorney-General*, above n 97, at [39], [45] and [56] to [67].

99 *Kyung Yup Kim v Minister of Justice and the Attorney-General*, above n 97, at [70].

100 *Kyung Yup Kim v Minister of Justice and the Attorney-General*, above n 97, at [275.b].

101 *Kyung Yup Kim v Minister of Justice and the Attorney-General*, above n 97, at [275.d].

102 *Kyung Yup Kim v Minister of Justice and the Attorney-General*, above n 97, at [275.f(i) to (v)].

consideration of any actions by the country taken in response to previously critical external reports); [103]

- whether the assurances are specific or are general and vague;[104]
- who has given the assurances and whether that person can bind the receiving State;[105]
- if the assurances have been issued by the central government of the receiving State, whether regional authorities can be expected to abide by them;[106]
- whether the assurances concern treatment which is legal or illegal in the receiving State;[107]
- the length and strength of bilateral relations between the sending and receiving States, including the receiving State's record in abiding by similar assurances;[108]
- whether the individual has previously been ill-treated in the receiving State;[109]
- whether compliance with the assurances can be objectively verified through diplomatic or other monitoring mechanisms;[110] including providing unfettered access to the individual's lawyer;[111] and to the individual themselves;
- whether there is an effective system of protection against torture in the receiving State, including a willingness to cooperate with international monitoring mechanisms (including UN special procedures and international human rights NGOs);[112]
- whether the State is willing to investigate allegations of torture and to punish those responsible;[113]

---

103 *Othman (Abu Qatada) v United Kingdom* (Application No. 8139/09) ECHR, 17 January 2012 (*Othman*) at [188]; Anderson and Walker *Deportation with assurances,* above n 90, at 49, noting this as "the key consideration to be taken into account when developing safety on return processes".

104 *Othman,* above n 103, at [189(ii)] citing *Saadi v Italy* (GC) no 37201/06 ECHR 2008.

105 *Othman,* above n 103, at [189(iii)] citing, *inter alia, Baysakov and Others v Ukraine* (54131/08) ECHR 18 February 2010 at [51]; *Soldatenko v Ukraine* (2440/07) ECHR 23 October 2008 at [73].

106 *Othman,* above n 103, at [189(iv)] citing *Chahal v United Kingdom* 15 November 1996 *Reports of Judgments and Decisions 1996-V* at [105] to [107].

107 *Othman,* above n 103, at [189(v)] citing, *inter alia, Cipriani v Italy* (221142/07) ECHR 30 March 2010; *Suresh v Canada (Minister of Citizenship and Immigration)* [2002] 1 SCR 3.

108 *Othman,* above n 103103, at [189(vii)] citing, *inter alia, Al-Moayad v Germany* (35865/03) ECHR 20 February 2007 at [68].

109 *Othman,* above n 103, at [189(ix)] citing, *inter alia, Koktysh v Ukraine* (43707/07) ECHR 10 December 2009 (*Koktysh v Ukraine)* at [64].

110 UK Intelligence Services Commissioner *Report of Intelligence Services Commissioner for 2015* (House of Commons, HC 459, 2016) at 43.

111 *Othman,* above n 103, at [189(viii)] citing, *inter alia, Chentiev and Ibragimov v Slovakia* (21022/08 and 511946/08) ECHR 14 September 2010.

112 *Othman,* above n 103, at [189(ix)] citing, *inter alia, Koktysh v Ukraine,* above n 109, at [63].

113 *Othman,* above n 103, at [189(ix)] citing, *inter alia, Koktysh v Ukraine*, above n 109, at [63].

- whether the reliability of the assurances has been examined by the domestic courts of the sending State;[114]

For assurances in general:

- whether the assurances are in writing or, at a minimum, a written record of an oral agreement;[115]

- whether a package of assurances can be delivered more satisfactorily through a collective MOU, than an individually tailored arrangement;[116] and

- whether there are clear and effective steps in place to take in case of suspected breach of the assurance.

74. In Canada, SIRC's *2017-2018 Annual Report* notes results from a further review of CSIS information sharing with foreign entities, in cases where the potential for mistreatment existed.[117] SIRC states that where mitigation measures were used (generally caveats and assurances), the associated risks should be appropriately assessed and documented.

> "The reliability of assurances to mitigate the risk of torture of mistreatment depends on a number of contextual factors. SIRC considered the following to be the most important: (1) the human rights record of the state and agency in question; (2) the length and strength of bilateral relations between the two states; and (3) the other state's record in abiding by assurances in the past."[118]

75. SIRC found that in two of the four case studies reviewed in 2017 the risks of sharing or soliciting information, as well as the risk that caveats and assurances would not be respected, were not appropriately assessed or documented by operational managers. At the strategic level, emphasising the importance of established requirements for monitoring and review, SIRC found that:

> "CSIS did not have any documented criteria or thresholds that would trigger a re-evaluation of the relationships with these countries in response to intelligence suggesting that assurances were not being adhered to."[119]

Mitigation tool: Legal initiatives

76. Legal initiatives can be engaged in order to understand a recipient State's interpretation of the law. This may seek to build a common understanding of international law and, where there are differences, to explore whether such interpretive differences can be bridged or managed,

---

114 MFAT *Expulsion with Diplomatic Assurances in the Context of Torture and Ill-Treatment* (DATE) citing *Othman,* above n 103, at [189(xi)] citing in turn, *inter alia, Babar Ahmad and Others v United Kingdom* (24027/07, 11949/08 and 36742/08) ECHR 6 July 2010 at [106].

115 UK Intelligence Services Commissioner *Report for 2015*, above n 110, at 43, regarding best practice for UK intelligence services when sharing intelligence with liaison partners and using assurances to mitigate against CIDT. Further, the UK Consolidated Guidance (2019) above n 54, at [21], requires that "[W]hen an assurance or caveat is not made in writing, personnel must keep an accurate record of any discussions and, whenever feasible, should share it with the foreign authority as a formal note as soon as is practicable."

116 Anderson and Walker *Deportation with assurances*, above n 90, at [7.5].

117 SIRC *2017-2018 Annual Report* (2018) at 15 to 17. This followed a first review by SIRC in 2015.

118 SIRC *2017-2018 Annual Report*, above n 117, at 16.

119 SIRC *2017-2018 Annual Report*, above n 117, at 17.

for example through the use of conditions, assurances and independent monitoring.[120] Where there are concerns about the recipient State's compliance with international law, it will be for the New Zealand government, as a matter of foreign policy, to decide how to respond.

Mitigation tool: Practising segmented cooperation or confining assistance to particular parts of a State

77. Where intelligence and security agencies hold concerns about particular agencies within a State, they may elect in future to share information only with specific parts of the State, or they may assess the risk to be lower if exchanging only specific types of information. This might comprise, for example, sharing 'building block intelligence' which contributes to a picture of a terrorist group over time, but not 'actionable intelligence' which may be more specific to individuals and thus more capable of giving rise to a breach of international law.[121]

Consider establishing a separate evaluative body

78. The practice of referring certain decisions on cooperation to an external or cross-government body for approval ensures transparent, robust and documented decision-making, and avoids the risk that agencies may conflate their operational or relationship objectives with the quite separate question of whether particular information sharing or cooperation is lawful or proper in any one case.

79. It can also afford some practical utility. A cross-government perspective can avoid inconsistencies (such as continuing cooperation in intelligence matters at a time when other cooperation is suspended). An external agency can bring a differently-informed perspective to an assessment of a receiving State or agency.

80. Under the CSIS MD, if there is a substantial risk of mistreatment in a given instance of information sharing and it is unclear whether that risk can be mitigated, the decision is referred to the Director of CSIS. This is automatically done via an Information Sharing Evaluation Committee (ISEC). Members of ISEC are senior CSIS officials and representatives from other government departments.[122] Before making a decision, ISEC guidelines indicate it can request additional checks such as carrying out a specific interview, or asking the foreign entity for details regarding how the information was obtained, in addition to usual check on the entity's human rights records and so forth.[123]

81. For the New Zealand Intelligence Community, the 'national security governance structures' outlined in Part 2 of the *National Security System Handbook*, suggest potential options for establishing a similar evaluative committee in New Zealand.

---

120 Harriet Moynihan "Aiding and Assisting: Challenges in Armed Conflict and Counterterrorism" (Research paper, International Law Programme, Chatham House 2016) citing Brian Egan "International Law, Legal Diplomacy, and the Counter-ISIL Campaign" (ASIL Conference, Washington DC, 1 April 2016) at 10 to 11.

121 On this distinction for sharing purposes, see Sir Peter Gibson *The Report of the Detainee Inquiry* (December 2013, at [4.15]; also UK Intelligence Services Commissioner *Supplementary to the Annual Report for 2015*, above n 43, at [21.3(2)], citing the approach taken in the OSJA *Human Rights Guidance.*

122 SIRC A*nnual Report 2017-18*, above n 117, "Case Studies Regarding CSIS Information Sharing with Foreign Entities".

123 Released under the Access to Information Act (to Craig Forcese; The Canadian Press).

Act lawfully and with propriety where a substantial/real risk of torture or CIDTP exists

82. Only after identifying likely or factual circumstances, assessing the risk, and, if necessary, considering options for mitigation, should a decision be taken on whether to proceed with the intelligence exchange or proposed assistance (eg at a detainee interview). If, despite taking appropriate steps in mitigation, there remains a real risk of torture, then best practice dictates that the exchange or cooperation should not proceed. The information sharing or participation in a detainee interview should be suspended, deferred or cease altogether.

> "Quite apart from the political and reputational risks involved, to proceed with assistance in the knowledge of noncompliance with international law by the recipient State entails responsibility under international law for the assisting State."[124]

83. The UN Special Rapporteur's Report on best practice states that "for sharing information about specific individuals, unsurprisingly the advice is to maintain an absolute prohibition on the sharing of any information if there is a reasonable belief that sharing information could lead to the violation of the rights of the individual(s) concerned".[125] This stance reflects that the condemnation of torture does not simply operate as an exclusionary rule of evidence, but is more aptly categorised as a constitutional principle.[126]

84. The UK's updated *Consolidated Guidance* requires, in situations where a real risk of torture exists, that any incidence of failure to comply with the *Guidelines* be reported to the oversight body, the Investigatory Powers Commissioner as soon as reasonably practicable after the event.[127]

Have in place robust monitoring, regular reviews and adequate record-keeping

Robust monitoring and regular review of State/agency actions

85. A country's record on human rights requires regular as well as responsive review. Monitoring developments in other jurisdictions must include measuring the extent to which recipient States comply with caveats and assurances and, as necessary, access to detainees remains open. As noted above, SIRC's review of information sharing arrangements found a State's failure to adhere to assurances to be a trigger for review. Current litigation in the UK has identified a concern that the Government may have relied upon assurances, despite UK intelligence agencies having, but not disclosing, information that undermined those assurances.[128]

86. If reviews, monitoring or other follow-up actions give rise to serious concerns about the compatibility of the actions of the recipient State or agency with the international law, best practice should dictate that the agency inquires into any alleged torture or ill-treatment of

---

124 Harriet Moynihan "Aiding and Assisting: Challenges in Armed Conflict and Counterterrorism", above n 120.

125 Martin Scheinin *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* A/HRC/10/3 (2009) at [47].

126 *A (No 2)*, above n 33, at [12] per Lord Bingham.

127 UK *Consolidated Guidance)* (2019) above n 54 at [22] to [29]. The procedures set out in the *Guidance* apply notwithstanding an authorisation granted under section 7 of the Intelligence Service Act 1994.

128 *Kamoka & Ors v Security Services & Ors* [2017] EWCA Civ 1665 at [99] and [115].

individuals. The results of these inquiries will contribute to the reassessment or final decision on whether it is lawful to exchange information.

Regular review of policy: Content and compliance

87. A process of regular review must include an agency's own policy, to ensure it adequately equips staff to consider and respond to risk, and make certain it is being complied with. In the UK, the UK *Consolidated Guidance* was reviewed in 2016 by the (former) Intelligence Services Commissioner, Rt Hon Sir Mark Waller. In 2018 the ISC summarised current issues with its breadth of application and content, including that it actually provides little specific guidance and that in the seven years it has been in place:

> "there appears to have been remarkably little attempt to evaluate or review its operation beyond ensuring compliance for oversight purposes. … While the Investigatory Powers Commissioner considers compliance with the Guidance, it is not his responsibility to consider whether the Guidance is achieving its policy objectives".[129]

88. As a result, the UK Prime Minister instructed the Investigatory Powers Commissioner (IPCO) to undertake a review of the *Consolidated Guidance*. As part of that review IPCO commenced a consultation round with civil society on 20 August 2018 (with the updated *Consolidated Guidance* published in July 2019). The publication of the relevant Guidance and public consultation as to content is a model that New Zealand should consider. Such transparency serves to emphasise the need for regular review of keep an agency's policy content fit for purpose.

Adequate record–keeping

89. The routine creation of an auditable trail of documents, recording the decisions and activities of intelligence services and their partners, is essential to both their internal operation and management and their external oversight.[130]

90. The former UK Intelligence Services Commissioner recommended the establishment of a central record–keeping hub which tracks and monitors all relevant allegations of torture and cruel, inhuman or degrading treatment or punishment, unlawful arrest or detention and procedural unfairness, and the steps taken in response.[131] In many respects this reflects the best practice noted above of a library of previous assessments and links to sources.

SUMMARY: THE ELEMENTS OF BEST PRACTICE

Clear Ministerial Directions:

- Set out the Minister's expectations and guidance to staff so that information sharing and cooperation by the intelligence and security agencies avoids any connection with acts of torture or CIDTP by other States and agencies;

129 UK ISC *Current Issues*, above n 66, at 1 and 2.
130 UK Intelligence Services Commissioner *Supplementary to the Annual Report for 2015*, above n 43, at [22.1].
131 UK Intelligence Services Commissioner *Supplementary to the Annual Report for 2015*, above n 43, at [21.3(5)].

- Clarify the exceptional circumstances, if any, in which the Minister considers that information likely obtained by torture may be used by the agencies and, if so, the constraints around such use.

Applicable law in a standalone guide for staff:

- Provide relevant domestic and international law on human rights, data protection and IHL.

Written formal arrangements/agreements on information sharing between parties (ie, between States or State agencies):

- Have clear rules governing the use of shared information, signed off by the Director of the intelligence and security agency or Minister;
- Include statements of compliance with human rights law, data protection obligations, and with the third party rule;
- Address situations where receipt is at third hand, and allow for the sending party to request feedback on use of the information;
- Ensure regular review, including by oversight bodies when arrangements/agreements are concluded or revised.

Policy to inform the assessment of a State's human rights record and risks around engagement:

- Provide a range of sources for information about States' human rights records and practices, including the treatment of detainees, and require assessments to be comprehensive by drawing on multiple sources of information;
- Be clear that making such assessments can involve asking hard questions, and that best practice should dictate an inquiry into allegations of torture or ill-treatment;
- Consider the nature of the information to be sent or received and the particular circumstances;
- Assess the likelihood of a real/substantial risk of human rights breaches;
- Include templates to guide making these assessments; and
- Ensure that information received unsolicited or "passively" by agencies also undergoes the requisite risk assessment as to whether it has likely been obtained by torture.

Take action to mitigate the risk of contributing to acts of torture:

- Employ caveats to set conditions (originator control) on how information may be used by the receiving party (or parties): in writing; establish procedures to monitor adherence to caveats by the receiving party; not appropriate as a sole method to mitigate risk or for a State/agency where caveats previously breached or with a poor human rights record;
- Seek assurances: in writing or at least a written and shared record of an oral undertaking; of sufficient detail; able to be monitored for compliance (for example, through right of access to a detainee); not appropriate as a sole

method to mitigate risk or for a State/agency where assurances previously breached or with a poor human rights record;

- Use legal initiatives: to, for example, build a common understanding with partners of obligations under international law;
- Practise segmented cooperation or confine assistance to particular parts of a State; or distinguish between 'actionable' and 'building block' intelligence.

Where there is a real/substantial risk of torture, ensure agency responses are lawful and proper:

- Have a plan in place for, when necessary, the immediate cessation of information sharing and cooperation with a State/agency, pending further inquiry;
- The plan should include seeking legal advice, informing the relevant Minister and oversight body.

Establish regular and responsive monitoring and review:

- Regularly review a State or foreign agency's human rights record and practices (including a State's legal approach to prohibiting acts of torture); trigger reviews in response to indications of human rights breaches; practice due diligence;
- Periodically monitor State/agency compliance with caveats, assurances and other undertakings;
- Regularly review policy content and your own agency's compliance with policy.

Require adequate record-keeping:

- Ensure adequate and informative records are available if decisions, in particular any relating to torture-derived information, are to be revisited or reviewed, and to facilitate effective democratic oversight.