National Security and Intelligence Review Agency

Office de surveillance des activités en matière de sécurité nationale et de renseignement

~~SECRET~~

REVIEW OF DEPARTMENTAL FRAMEWORKS FOR AVOIDING COMPLICITY IN MISTREATMENT BY FOREIGN ENTITIES

(NSIRA REVIEW 2019-06)

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
Tel: *1-833* 890-0293 Fax: *613* 907-4445

I EXECUTIVE SUMMARY 1
II AUTHORITIES 6
III INTRODUCTION 6
IV BACKGROUND 7
V OBSERVATIONS AND RECOMMENDATIONS 9
Reporting 9
Implementation of the 2017 Ministerial Direction 10
Independent Decision-Making 13
Country Assessments 15
Duty of Care 16
Substantial Risk 17
VI CONCLUSION 18
ANNEX A: Scope and Methodology 19
ANNEX B: Meetings and Briefings 20
ANNEX C: Recommendations 21
ANNEX D: Communications Security Establishment 22
ANNEX E: Royal Canadian Mounted Police 28
ANNEX F: Canadian Security Intelligence Service 36
ANNEX G: Department of National Defence and the Canadian Armed Forces 46
ANNEX H: Global Affairs Canada 54
ANNEX I: Canada Border Services Agency 60

I EXECUTIVE SUMMARY

1. In 2011 and again in 2017, ministers issued direction (hereafter Ministerial Direction or MD) to a number of departments setting out how to manage the risks of mistreatment posed by the sharing of information with foreign entities. Most recently, Parliament passed the *Avoiding Complicity in Mistreatment by Foreign Entities Act* (ACMFEA). In September 2019, direction under the ACMFEA was issued to twelve departments, six of which had never before received formal direction regarding information sharing with foreign entities.

2. This review set out to build NSIRA's knowledge of the information sharing processes adopted by departments under the 2017 MD. The direction issued pursuant to the ACMFEA in September 2019 codified many provisions of the 2017 MD and left the essential prohibitions and limits unchanged. As such, this review provided a foundation that will expedite and facilitate NSIRA's future information sharing reviews.

3. The review focused on the six departments that had received the 2017 MD: the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment (CSE), the Royal Canadian Mounted Police (RCMP), the Canada Border Services Agency (CSBA), Global Affairs Canada (GAC), and the Department of National Defence and the Canadian Armed Forces (DND/CAF).

Observations and Recommendations

Degrees of implementation vary across departments

4. NSIRA noted significant differences between the six departments with regard to the level of implementation of information sharing processes. In summary:

- CSE, CSIS and the RCMP have implemented the 2017 MD.
- DND/CAF is in the process of implementing final elements of the 2017 MD.
- GAC has not yet fully implemented the 2017 MD.
- In practice, CBSA has not yet operationalized the 2017 MD.

The concept of "substantial risk" of mistreatment is not defined

5. Like the 2017 MD, the ACMFEA and its associated direction prohibit information sharing that would result in a "substantial risk" of mistreatment. Neither the ACMFEA nor its direction include a definition of substantial risk, however, despite the centrality of this concept to the regime. A definition of substantial risk existed in both the 2011 and

2017 MD; its absence now raises concerns about its interpretation in future.

Recommendation: The definition of "substantial risk" should be codified in law or public direction.

Departments vary with respect to the independence of their decision-making

6. NSIRA examined the extent to which high-risk decision-making is removed from operational personnel who may have a vested interest in the sharing. In some departments, the decision-makers have a direct operational interest in the sharing of information, creating the potential for conflict between operational imperatives and departmental obligations to respect the MD. In particular, NSIRA noted that:

- CSE and the RCMP have the most independent processes.
- The information sharing processes implemented by GAC to date remove high-risk decision-making from "front line" personnel.
- At CSIS and DND/CAF, decision-makers typically have a direct operational interest in the sharing of information.
- CBSA has not yet operationalized its information sharing processes.

Recommendation: Departments should ensure that in cases where the risk of mistreatment approaches the threshold of "substantial", decisions are made independently of operational personnel directly invested in the outcome.

Lack of standardized information sharing risk assessments

7. Under the 2017 MD, GAC, CSIS, CSE, and the RCMP all maintain their own sets of foreign country and/or entity profiles, while DND/CAF is currently developing its own as well. The existence of multiple different assessments is duplicative and unnecessary. It may also yield inconsistencies, as departments have at times come to quite different conclusions about foreign countries' and entities' human rights records and the associated risks of information sharing.

Recommendation: Departments should develop: (a) a unified set of assessments of the human rights situations in foreign countries including a standardized 'risk of mistreatment' classification level for each country; and (b) to the extent that multiple departments deal with the same foreign entities in a given country, standardized assessments of the risk of mistreatment of sharing information with foreign entities.

Benefits of internal information sharing process reviews

8. Finally, NSIRA noted that periodic internal reviews of information sharing policies and processes supported their successful functioning in the long term.

Recommendation: Departments should conduct periodic internal reviews of their policies and processes for sharing information with foreign entities in order to identify gaps and areas in need of improvement.

II AUTHORITIES

9. This review was conducted under the authority of the *National Security and Intelligence Review Agency Act* (*NSIRA Act*), specifically paragraphs 8(1)(a) and 8(1)(b) as well as sections 9 and 11.

III INTRODUCTION

10. Many departments and agencies[1] in the Government of Canada routinely share information with foreign entities. Given that information sharing with entities in certain countries can result in a risk of mistreatment for individuals, it is incumbent upon the Government of Canada to evaluate and mitigate the risks that such sharing creates. This is particularly the case for information sharing related to national security and intelligence, where the information often relates to alleged participation in terrorism or other criminal activity.

11. Canada has made a number of binding commitments under the *International Covenant on Civil and Political Rights* (ICCPR),[2] the *Convention Against Torture and Other Cruel, Inhumane, or Degrading treatment or Punishment* (CAT), and other international agreements. The prohibitions on mistreatment – including complicity in mistreatment – set out in these agreements are also considered to be customary international law. Some of Canada's obligations have been incorporated into domestic law under section 269.1 of the *Criminal Code*.[3]

12. In 2011 and again in 2017, ministers issued direction to a number of departments setting out how to manage the risks in information sharing with foreign entities.[4] Most recently, Parliament passed Bill C-59, which included the ACMFEA. In September 2019, direction under the ACMFEA was issued to twelve departments, six of which had never before received formal direction regarding information sharing with foreign entities.

13. Subsection 8(2.2) of the *NSIRA Act* requires NSIRA to review annually every department's implementation of the directions of the GiC issued under the ACMFEA. In 2020, the NSIRA will undertake its first such review. The purpose of the present review, however, was to build NSIRA's knowledge and understanding of departments' implementation of the 2017 MD. The direction issued pursuant to the ACMFEA in

---

[1] Hereafter referred to simply as "departments" for ease of reading.
[2] Article 7 states that "no one shall be subjected to torture or cruel, inhumane or degrading treatment or punishment".
[3] The prohibition on the use of evidence derived from torture is also noted in the *Immigration and Refugee Protection Act*.
[4] The 2017 MD defines "mistreatment" to mean "torture or other cruel, inhuman, or degrading treatment or punishment".

September 2019 codified many provisions of the 2017 MD and left the essential prohibitions and limits unchanged. As such, this review provided a valuable foundation that will expedite and facilitate NSIRA's future information sharing reviews.

14. The review focused on the six departments that received the 2017 MD: CSIS, CSE, the RCMP, CBSA, GAC, and DND/CAF. NSIRA examined departments' policies and processes as well as documents related to foreign arrangements. Where possible, NSIRA examined a single case study for each department in order to illustrate how information sharing works in practice.[5] Given the high-level approach taken in this review, NSIRA opted to make a series of broad observations about the strengths and weaknesses of departments' framework for information sharing with foreign entities, in the place of formal findings. Where NSIRA made recommendations, they were interdepartmental in scope.

15. This review focussed on departmental policies and procedures for the *disclosure* and *requesting* of information involving a risk of mistreatment. It did not examine the *use* of information that may have been derived from mistreatment; NSIRA may review this topic in future.[6]

IV BACKGROUND

16. In 2011, the Government of Canada approved a general framework for "Addressing Risks of Mistreatment in Sharing Information with Foreign Entities". The framework was the first multi-departmental set of instructions issued regarding information sharing and mistreatment. Its main aim was to establish a coherent and consistent approach across government when sharing information with foreign entities.

17. Later in 2011, a number of departments whose mandate related to national security and/or intelligence received *Ministerial Direction on Information Sharing with Foreign Entities* (the 2011 MD). Specifically, the 2011 MD was issued to CSIS, CSE, CBSA, and the RCMP. The 2011 MD, which was eventually released under the *Access to Information Act*, was subject to extensive criticism from non-governmental

[5] NSIRA chose a case from 2018 or 2019 that had not yet been subject to review. Cases were chosen because they demonstrated each department's complete process for assessing the risks of mistreatment.
[6] Both the 2017 Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities and the direction issued under the ACMFEA provide distinct guidance regarding the use of information derived from torture. Specifically, such information may not be used: (a) where it creates a substantial risk of further mistreatment; (b) as evidence in any judicial, administrative or other proceeding; or (c) in any way that would deprive someone of their rights or freedoms, unless it is determined that the use of the information is necessary to prevent a loss of life or significant personal injury.

organizations, civil liberties groups, and others including the Canadian Bar Association.[7] The main critique was that the 2011 MD did not clearly prohibit the disclosure or requesting of information entailing a "substantial risk" of mistreatment, but rather permitted departments to weigh the value of the information against the risk of mistreatment.[8]

18. In 2017, the 2011 MD was replaced by a new *Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities* (the 2017 MD). The 2017 MD was received by CSIS, CSE, CBSA, and the RCMP – the departments that had received the 2011 MD – as well as by DND/CAF and GAC. The 2017 MD included numerous changes, but the most significant were clear prohibitions on the disclosure and requesting of information that would result in a substantial risk of mistreatment,[9] as well as new limits on the use of information likely derived from mistreatment by a foreign entity. In addition, the new MD required departments to maintain policies and procedures to assess the risks of their information sharing relationships with foreign entities.

19. The 2017 MD further directed departments to cooperate in making assessments regarding foreign countries and entities.[10] In response, Public Safety Canada (PS) established the Information Sharing Coordination Group (ISCG) comprised of PS and the six departments that had received the 2017 MD. The objective was to encourage interdepartmental discussions in support of a coordinated approach to the implementation of the MD.[11]

20. On July 13, 2019, the ACMFEA came into force. The ACMFEA requires the GiC to issue direction to the six departments that had received the 2017 MD, and gives the GiC discretion to issue direction to other departments as well. On September 4, 2019, the GiC issued direction under the ACMFEA to twelve departments. In addition to the six mandatory departments, direction was issued to PS; the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC); Transport Canada; Immigration, Refugees and Citizenship Canada (IRCC); the Canada Revenue Agency (CRA); and

---

[7] Examples include the Amnesty International letter to the Minister of Public Safety: Canada must withdraw Ministerial Direction on information sharing with foreign entities tainted by torture, March 6, 2012; the Canadian Bar Association: Resolution 13-08-A, Ministerial Direction on Information Sharing with Foreign Entities, August 17, 2013; and the Canadian Civil Liberties Association Report to the UN Human Rights Committee, 114 Session June 2015, pg.14.
[8] Under the 2011 MD, the "approval level that CSIS requires in order to share information must be proportionate to the risk of mistreatment that may result: the greater the risks the more senior the level of approval required".
[9] The 2017 MD defined "substantial risk" as "a personal, present and foreseeable risk of mistreatment. In order to be 'substantial', the risk must be real and must be based on something more than mere theory or speculation. In most cases, the test of substantial risk of mistreatment will be satisfied when it is more likely than not that there will be mistreatment; however, in some cases, particularly where there is risk of severe harm, the 'substantial risk' standard may be satisfied at a lower level of probability".
[10] The 2017 MD required departments to "cooperate in this assessment process with all other Government of Canada departments and agencies covered by the Ministerial Direction to ensure that decision making is supported by the most comprehensive assessment base of information possible".
[11] Public Safety Canada briefing to NSIRA, September 30, 2019.

Fisheries and Oceans Canada (DFO). These six new departments have now also joined the PS-led ISCG.

21. In practice, the information sharing regime set out by the ACMFEA and the subsequent GiC direction closely resembles the 2017 MD. The fundamental limits on Canadian departments' scope to share information remain unchanged. Notably, however, the new regime omits certain aspects of the 2017 MD. The ACMFEA and its associated direction lack the 2017 MD's requirement that departments maintain policies and procedures for assessing the risks associated with foreign information sharing arrangements, in collaboration with other departments. More importantly, the new system omits a definition of the threshold of "substantial risk". The ramifications of this are discussed below.

V OBSERVATIONS AND RECOMMENDATIONS

Reporting

22. One of the new obligations placed on departments in the 2017 MD was a requirement that they provide an annual report to their minister that included:

- the details of "substantial risk" cases where the MD was engaged, including the number of such cases;
- restrictions on any foreign arrangements put in place due to concerns related to mistreatment; and
- any changes to internal policies and procedures related to the 2017 MD.

Departments were also directed to release publically an unclassified version of the report.

23. All of the departments that were issued the 2017 MD fulfilled their obligation to report to their respective ministers by producing a report in late 2018 or early 2019 discussing the first year of activity under the MD. At the time of writing, however, not all of the departments have issued a public report. As this was a foundational review, NSIRA did not critically evaluate the reports.

Departmental Reporting (2017 MD)

Department	Report to Minister	Public report	Cases approved	Cases denied
CBSA	Provided	Published	0	0
CSIS[12]	Provided	Published	1	1
RCMP[13]	Provided	Published	25	4
CSE[14]	Provided	Published	1	0
DND/CAF	Provided	Not Published	0	0
GAC	Provided	Not Published	0	0

Implementation of the 2017 Ministerial Direction

24. When the 2017 MD was issued, departments that had already built information sharing policies and procedures under the 2011 MD found themselves at a significant advantage. CSIS, CSE, and the RCMP in particular were able to quickly adapt their existing systems to the 2017 MD. Accordingly, for departments that had not received the 2011 MD – or had not implemented it – the arrival of the 2017 MD proved more challenging.

25. **CSE: NSIRA observes that CSE has fully implemented all of the elements of the 2017 MD.** The MD's requirements have been integrated directly into CSE's operational policies and processes.[15] A detailed overview of CSE's information sharing framework and the results of the case study examined by NSIRA can be found at **Annex D**.

26. **RCMP:** In response to the 2017 MD, the RCMP overhauled their information sharing framework and stood up a new Law Enforcement Assessment Group (LEAG) that, amongst other things, assesses country human rights records and maintains a system for streaming information sharing requests according to risk.[16] The RCMP is currently working to integrate these processes into their comprehensive operational manual. A detailed overview of the RCMP's information sharing framework and the results of the case study examined by NSIRA can be found at **Annex E**.

---

[12] ISEC considered cases that involved substantial risk of mistreatment, of which were referred to the Director of CSIS.
[13] The RCMP numbers reflect the number of cases before the Foreign Information Risk Advisory Committee (FIRAC), discussed below. All of FIRAC's recommendations are endorsed or denied by an Assistant Commissioner and are thus deemed by the RCMP to fall within the reporting requirements of the 2017 MD.
[14] The Chief of CSE determined that the risk of mistreatment was mitigated by several factors and approved one case for sharing.
[15] Mission Policy Suite: Authorities, Governance and Accountability, April 2, 2019, Mission Policy Suite A, Standards of Operating Procedures.
[16] RCMP Implementation of the Avoiding Complicity in Mistreatment by Foreign Entities Act: Briefing to NSIRA, October 3, 2019.

27. **CSIS:** Following the issuance of the 2017 MD, CSIS quickly updated their policies and procedures. In 2018, CSIS also created a new system to implement the MD's requirement to restrict information sharing with foreign entities that engage in mistreatment, with three levels of restriction depending on the seriousness of the problem. CSIS has informed NSIRA that it is overhauling its current policies and procedures. A detailed overview of CSIS's current information sharing framework and the results of the case study examined by NSIRA can be found at **Annex F**.

28. **DND/CAF:** Although DND/CAF did not receive the 2011 MD, DND/CAF has had internal directives in place governing information sharing with foreign entities since 2010.[17] The DND/CAF policy and process suite for information sharing was updated following the issuance of the 2017 MD to bring it into compliance with the new requirements.[18] While DND/CAF vets partner forces, it does not yet have a fully developed system for assessing and managing the risks of sharing information with foreign entities.[19] DND/CAF is, however, currently developing more extensive country risk profiles and a standardized assessment process that will be used to assess the risks of information sharing prior to establishing information sharing arrangements.[20] A detailed overview of DND/CAF's information sharing framework can be found at **Annex G**.

29. **GAC:** Following receipt of the 2017 MD, GAC established a new Ministerial Direction Compliance Committee (MDCC) in December 2018. The MDCC's objective is to review requests for information sharing that may engage the MD.[21] This is the extent of GAC's policies and processes pursuant to the MD, however. GAC lacks any policies or procedures setting out how employees are to assess instances of possible information sharing to ensure that all appropriate cases reach the MDCC. It is insufficient to merely inform employees that they are responsible for assessing a complex legal threshold – the concept of a "substantial risk" of mistreatment at the core of the 2011 and 2017 MD as well as the ACMFEA – without guidance as to how they should proceed. As such, **NSIRA observes that GAC has not yet fully implemented the 2017 MD**.

30. **GAC (cont.):** Of note, GAC produces human rights reports on countries that are

---

[17] CDI Functional Directive on Intelligence and Intelligence Derived Information Sharing with Foreign Entities, June 14, 2010.
[18] The DM/CDS Directive on the Disclosure, Request and Use of Information: Avoiding Complicity in Mistreatment by Foreign Entities issued on April 2018.
[19] Chief of Defence Intelligence: Interim Functional Directive: Information Sharing with Certain Foreign States and Their Entities: Annex A: Foreign States with Low Risk of Engaging in Mistreatment. April 20, 2019.
[20] E-mail responses to NSIRA, MD on Avoiding Complicity in Mistreatment by Foreign Entities (NSIRA 2019-02), October 11, 2019.
[21] Term of Reference – Committee on Compliance with Ministerial Direction to Global Affairs Canada: Avoiding Complicity in Mistreatment by Foreign Entities ("Ministerial Direction Compliance Committee").

widely used within government to assist in assessing the risks of sharing with foreign entities. Following the 2017 MD, GAC added a subsection specific to mistreatment to these reports.[22] A detailed overview of GAC's information sharing framework and the results of the case study examined by NSIRA can be found at **Annex H**.

31. **CBSA:** In October 2018, CBSA issued a revised high-level policy document in response to the 2017 MD. The document did not include concrete processes for identifying and handling instances of information sharing involving a risk of mistreatment, however. CBSA employees thus lack effective guidance with which to discharge their responsibilities under the MD. CBSA also has no process for assessing the risks associated with specific foreign countries and entities, as required by the MD. CBSA has since drafted processes and additional policies, but they have not yet been finalized or invoked. Given these significant gaps, **NSIRA observes that CBSA has not yet operationalized the 2017 MD**. CBSA has informed NSIRA, however, that it intends to introduce significant improvements over the coming year. A detailed overview of CBSA's information sharing framework can be found at **Annex I**.

32. Additional observations are included in the department-specific annexes referenced above. It should also be noted that NSIRA examined departmental policies and processes at a high level, and as such future reviews may make additional findings and recommendations regarding policies and processes. Moreover, a number of departments are in the process of revamping their information sharing practices, including in particular CSIS and DND/CAF.

33. In its survey of departments, NSIRA noted varying levels of rigour and consistency with regard to record keeping. Accurate and detailed records of deliberations and reasoning in support of decision-making related to information sharing with foreign entities are necessary to support accountability, particularly in light of the Supreme Court's recent decision in *Vavilov*.[23] NSIRA may return to this subject in future years.

34. In June 2019, the RCMP conducted an internal review of the framework and policies in place for its information sharing policies and procedures. The review identified certain shortcomings with regard to policies, processes, training, and resourcing. Based on the draft provided, **NSIRA observes that the review was candid and thorough.** The review is currently being used to guide improvements. Periodic internal reviews – such as the one conducted by the RCMP – should be considered a best practice.

---

[22] GAC Human Rights Reports Guidelines April 2018 – March 2019.
[23] *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65.

Recommendation no. 1: Departments should conduct periodic internal reviews of their policies and processes for sharing information with foreign entities in order to identify gaps and areas in need of improvement.

Independent Decision-Making

35. The concept of risk mitigation is key to the information sharing frameworks of departments. When information sharing would result in a substantial risk that an individual would be mistreated, the information can only be shared if the department takes measures to mitigate the risk of mistreatment such that the residual risk is no longer substantial. Much therefore depends on who, within departments, is authorized to make decisions regarding whether:

(a) an instance of proposed information sharing would result in a substantial risk of mistreatment; and

(b) the proposed mitigation measures are sufficient.

36. In looking at the various decision-making processes adopted by departments, NSIRA noted varying levels of independence from operational personnel. Of particular interest were processes where the individual making decisions has a direct operational interest in the sharing of the information, creating the potential for conflict between operational imperatives and departmental obligations to respect the MD.

37. At CSE, the complete Mistreatment Risk Assessment process is conducted by non-operational units.[24] The centralization of information sharing decision-making in a single branch minimizes direct operational pressure while facilitating informed and objective decisions.

38. The RCMP process uses other mechanisms to ensure independent decision-making. Individual investigators, when they wish to share information, must consult a list of countries and types of information sharing that the RCMP has pre-determined as representing sufficient risk of mistreatment. If the proposed sharing matches the list, then the case is automatically referred to the Foreign Information Risk Advisory Committee (FIRAC). FIRAC comprises a range of senior officials from RCMP

[24] Mistreatment Risk Assessment (MRA): is the tool used by CSE to assess the potential risk of mistreatment of individuals before sharing information, MRAs are informed by classified and open source information regarding the human rights country reporting as well as an assessment of the internal record/reporting of the foreign entity under consideration and an analysis of the risk mitigation measures available. See CSE's Application of the Ministerial Direction: Avoiding Complicity in Mistreatment by Foreign Entities- 2017-2018 Annual Report (unclassified report).

headquarters who are a step removed from the operational front-line. The RCMP's system of referral to FIRAC based on clear criteria removes discretion from officers with a vested interest in the sharing of the information. These officers may not have a full understanding of the geopolitical context of the proposed information sharing and thus are not best-placed to assess whether a substantial risk of mistreatment would result.

39. GAC requests that Directors General and Heads of Mission refer all cases where proposed information sharing "presents the potential for substantial risk of mistreatment" to the MDCC. The decision as to whether the substantial risk can be mitigated is made centrally by the MDCC, which comprises senior officials from across the department as well as a legal representative. As noted above, however, GAC currently does not provide officials with guidance on how to determine whether the threshold for referral to the MDCC has been met.

40. Compared to CSE, GAC, and the RCMP, decision-making at CSIS and DND/CAF is much closer to operations. CSIS provides high-level guidance to desks on how to identify information sharing that may result in a substantial risk of mistreatment, but leaves final decision-making regarding whether the situation does in fact create a substantial risk, and whether the risk can be mitigated, to the Deputy Director General or the Director General of each branch.[25] Only if CSIS has heavily restricted information sharing with the foreign entity in question – or else the branch is *unsure* whether the substantial risk can be mitigated – then the branch must refer the case to the Information Sharing Evaluation Committee (ISEC) for determination. As a result, most of CSIS's information sharing decisions – even those involving a substantial risk of mistreatment – are made by officials with a direct operational stake in the outcome of the proposed information sharing.

41. Within DND/CAF, decisions regarding the sharing of information rest with officers within the military chain of command. NSIRA was informed that while routine information sharing is approved by designated lower-level officers in theatre, cases involving unusual circumstances, or where there is uncertainty as to whether a substantial risk of mistreatment exists or can be mitigated, are elevated to senior levels. Once passed up the chain of command, senior officers receive advice from a range of officials at headquarters.

42. CBSA, at the present time, does not have processes to assess substantial risk or to make decisions regarding whether such risks can be mitigated. In practice, therefore, the onus currently rests on CBSA officers, acting without guidance, to identify cases that invoke the 2017 MD and to manage the associated risks. CBSA has drafted a procedure for cases where there is uncertainty as to whether a substantial risk of

[25] Memorandum: DDO Directive on Avoiding Complicity in Mistreatment by Foreign Entities, September 28, 2017.

mistreatment can be mitigated, but it has not yet been implemented.

Recommendation no. 2: Departments should ensure that in cases where the risk of mistreatment approaches the threshold of "substantial", decisions are made independently of operational personnel directly invested in the outcome.

Country Assessments

43. As noted above, a significant addition to the 2017 MD was the requirement that departments maintain policies and procedures to assess the risks of their information sharing relationships with foreign entities. Notably, the MD required departments to assess the human rights records of foreign countries generally and not just of specific foreign entities (i.e., police or intelligence services) within those countries.[26] While the MD did not prohibit information sharing with foreign entities in countries with troubling human rights records, it implied that Canada's relationships with such foreign entities could not be considered in isolation from the broader human rights environment in which these entities functioned.

44. In several instances, NSIRA noticed departments citing an absence of direct Government of Canada intelligence of mistreatment by a specific foreign entity in support of a proposed sharing of information, or else in support of a less restrictive information sharing policy towards the entity in question – despite ample reporting of systemic human rights abuses in the public domain.[27] **NSIRA observes that a lack of internal Government of Canada reporting of mistreatment by a specific foreign entity is not evidence that the entity does not engage in mistreatment.** Departments must consider the full range of sources in assessing risk, including open sources such as the media and non-governmental organizations.

45. GAC, CSIS, CSE, and the RCMP all maintain their own sets of foreign country and/or entity profiles, while DND/CAF is currently developing its own as well. The existence of multiple different assessments is duplicative and unnecessary. It may also yield significant inconsistencies, as departments have at times come to quite different conclusions about foreign countries' and entities' human rights records and the associated risks of information sharing. With the issuance of direction under the

[26] The 2017 MD states each department "will maintain internal policies and procedures for assessing the risks associated with relationships with foreign entities. This includes evaluating the human rights records of foreign governments generally, and not only the specific entities associated with them".
[27] In several instances, in was noted that departments dwelled on the extent of their internal knowledge of mistreatment by a specific foreign entity – despite extensive reporting by Human Rights Watch, Amnesty International, and/or other non-governmental organizations regarding the human rights situations in the country, including abuses by the local security and intelligence services.

ACMFEA to twelve departments, this issue will likely grow. See **Annex F** for additional discussion of this point.

46. The ISCG seeks to guide departments in developing their human rights assessment processes by providing a forum to discuss best practices. PS informed NSIRA that the ISCG had not discussed plans to standardize these assessments.

Recommendation no. 3: Departments should develop:

a) a unified set of assessments of the human rights situations in foreign countries including a standardized 'risk of mistreatment' classification level for each country; and

b) to the extent that multiple departments deal with the same foreign entities in a given country, standardized assessments of the risk of mistreatment of sharing information with foreign entities.

47. The recommendation above does not preclude department-specific approaches to mitigating the risks of mistreatment. For instance, a department may be able to draw upon aspects of its relationship with a foreign entity to reduce the risk of mistreatment not available to other departments. These differences should not affect the initial determination of the underlying risk of mistreatment posed by information sharing with a foreign entity, however.

48. In *India v. Badesha* (2017), the Supreme Court of Canada recently provided guidance on contextual factors to be considered when assessing the reliability of assurances sought from foreign entities regarding mistreatment.[28] Though not exhaustive, the decision provides departments with some guidance regarding the adequacy of assurances received.

Duty of Care

49. In reviewing GAC, NSIRA noted a tension between adherence to the 2017 MD and GAC's duty of care with regard to the safety and security of mission staff abroad. Indeed, both cases of information sharing referred to the MDCC in 2019 involved threats to mission security. In one of the cases, information was shared with a foreign entity before the MDCC had had the chance to assess the risk of mistreatment. In this instance, the GAC official cited the need to protect the safety of mission staff (see **Annex H**).

[28] *India v. Badesha*, 2017 SCC 44, [2017] 2 SCR 127.

50. NSIRA acknowledges the importance of mission security and the seriousness of the conundrums that can arise when the needs of mission security and GAC's obligations with respect to information sharing collide. Yet the charged atmosphere of a mission under threat may not be the best venue for quick decision-making involving risks of mistreatment.

Substantial Risk

51. Like the 2017 MD, the ACMFEA and its associated direction prohibit information sharing that would result in a substantial risk of mistreatment. Neither the ACMFEA nor its direction include a definition of "substantial risk", however, despite the centrality of this concept to the regime. A definition of substantial risk existed in both the 2011 and 2017 MD; its absence now raises concerns about its interpretation in the future.

52. In consultation with other departments, PS is developing a policy document that includes the same definition of substantial risk that was found in the 2011 and 2017 MD. The document also contains guidance on other requirements contained in the 2017 MD but that were omitted from the ACMFEA and its direction.[30] When asked by NSIRA, the six departments that had been subject to the 2017 MD all stated that they intended to continue abiding by the established definition of substantial risk.[31] This is reassuring, and should limit the potential for inconsistency between departments. Nonetheless, such a crucial definition should not be left up to individual departments to determine.

Recommendation no. 4: The definition of "substantial risk" should be codified in law or public direction.

53. The definition of substantial risk in the 2017 MD requires that mistreatment be "foreseeable". As described in **Annex G**, DND/CAF's assessment of foreseeability encompasses a number of factors, but a key component is that the risk of mistreatment be a "causal consequence" of DND/CAF information sharing.[32] **NSIRA observes that**

---

[30] PS draft document "Guidance on the Directions for Avoiding Complicity in Mistreatment by Foreign Entities".
[31] GAC stated that they would abide by the definition put forward by the ISCG, which is currently identical to that in the 2017 MD.
[32] DND/CAF has informed NSIRA that "for a risk to be considered foreseeable, the risk must be such that a reasonable person, with the reasonably available information at the time of sharing, would foresee mistreatment as a consequence of said sharing. Foreseeability is assessed based on all facts available at the time of sharing and must constantly be reassessed as situations change or new information is received. In addition, to be substantial, the risk

DND/CAF's interpretation of foreseeability runs the risk of narrowing the definition of substantial risk and therefore the application of the 2017 MD. Given the importance of a clear and consistent understanding of "substantial risk" across departments, in future years NSIRA may review the application of the "substantial risk" threshold by DND/CAF – and other departments – to information sharing with foreign entities.

54. A substantial risk of mistreatment is defined as existing in cases where mistreatment is more likely than not. The definition includes a qualifier, however, that the threshold may be met at lower level of probability "where the risk is of severe harm". This reflects a larger point that the assessment of substantial risk is not intended to be a narrowly mechanistic process of balancing probabilities. The 2017 MD notes that the Government of Canada "has no interest in actions associated with the use of torture or other cruel, inhumane or degrading treatment or punishment. Knowingly associating the Government of Canada with any of these actions would damage the credibility and effectiveness of any department or agency associated with them".[33] When interpreting the threshold of substantial risk, departments should always bear in mind the larger purpose of Canada's framework for sharing information with foreign entities.

55. In order to give life to this framework, it is incumbent on departments, first, to ensure that their employees are trained to the point where they fully understand their legal obligations, and second, to establish clear and well-developed processes that foster and facilitate compliance in the broadest sense.

VI CONCLUSION

56. This review set out to build NSIRA's knowledge of the information sharing processes adopted by departments under the 2017 MD. NSIRA noted significant differences between the six departments reviewed with respect to the level of implementation of information sharing processes. Processes also varied widely in terms of the level of independence of decision-making.

57. Although departmental information sharing frameworks will continue to evolve over time, this review will provide a baseline of comparison for future developments under the ACMFEA. The review also served to identify areas of potential concern that NSIRA may revisit in future years.

---

must be real based on something more than theory or speculation. To be foreseeable, the mistreatment must occur as a causal consequence of the sharing of information." *(emphasis added)* DND/CAF response to NSIRA draft report (consolidated comments table, page 3), February 5, 2020.

[33] Ministerial Direction: Avoiding Complicity in Mistreatment by Foreign Entities (s. 14 for CSE, CSIS, CBSA, the RCMP and s. 13 for GAC and DND/CAF).

ANNEX A: Scope and Methodology

This review examined the information sharing practices of the six departments in receipt of the 2017 MD (DND/CAF, GAC, CSIS, CSE, CBSA, and the RCMP).

NSIRA submitted several requests for information to the six departments. The documents requested pertained to the 2011 MD and the 2017 MD. NSIRA also requested documents from PS in relation to its leadership of the ISCG. The period of the review included January 2017 to September 2019, as well as 2011.

NSIRA reviewed departmental information sharing frameworks, including internal processes, procedures, policies, and legal opinions, particularly with regard to the implementation of the 2017 MD. Documents regarding the implementation of the 2011 MD provided insight into the evolution of departmental information sharing practices. Where applicable, NSIRA also reviewed changes that are anticipated as a result of the implementation of the ACMFEA.

For each of the six departments, whenever possible NSIRA chose one case study for deeper review. The case study was selected from a list of cases referred to senior management between 2017 and 2019. NSIRA examined official records, legal opinions and correspondence related to each case.

NSIRA received individual briefings from each department. NSIRA also received answers to follow-up questions secretarially and, in one instance, through an additional briefing.

ANNEX B: Meetings and Briefings

- CSE: September 10, 2019
- CSIS: September 12, 2019, and November 14, 2019
- DND: September 20, 2019, and February 10, 2020
- PS: September 30, 2019
- RCMP: October 3, 2019
- CBSA: November 1, 2019
- GAC: November 8, 2019, and February 12, 2020

ANNEX C: Recommendations

Recommendation no. 1: Departments should conduct periodic internal reviews of their policies and processes for sharing information with foreign entities in order to identify gaps and areas in need of improvement.

Recommendation no. 2: Departments should ensure that in cases where the risk of mistreatment approaches the threshold of "substantial", decisions are made independently of operational personnel directly invested in the outcome.

Recommendation no. 3: Departments should develop: (a) a unified set of assessments of the human rights situations in foreign countries including a standardized 'risk of mistreatment' classification level for each country; and (b) to the extent that multiple departments deal with the same foreign entities in a given country, standardized assessments of the risk of mistreatment of sharing information with foreign entities.

Recommendation no. 4: The definition of "substantial risk" should be codified in law or public direction.

ANNEX D: THE COMMUNICATIONS SECURITY ESTABLISHMENT

I BACKGROUND

1. In November 2011, the Communications Security Establishment (CSE) received the Ministerial Directive on the Framework for Addressing Risks in Sharing Information with Foreign Entities (the 2011 MD).[1]

Accordingly, the policies and procedures implemented by CSE during the years that followed focused on the risk of mistreatment

2. The CSE Mistreatment Risk Assessment (MRA) process that emerged was supported by detailed policies, procedures and templates. Nonetheless, responsibility for the process was divided between and the Corporate and Operational Policy Section . In 2017, the Office of the CSE Commissioner (OCSEC), CSE's external review body at the time, found that the two sections diverged in how they implemented the MRA process.[3] As a result, the branch of CSE was assigned sole responsibility for the MRA process, thereby consolidating the management of all disclosure requests into a single hub.

II THE 2017 MINISTERIAL DIRECTION

3. On October 25, 2017, CSE received the new Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities (the 2017 MD), which replaced the 2011 MD. Unlike in 2011, when CSE had received direction somewhat distinct from CSIS, RCMP, and CBSA, the 2017 MD issued to CSE was substantively identical to the MD

---

[1] Ministerial Directive: Communications Security Establishment: Framework for Addressing Risks in Sharing Information with Foreign Entities, November 21, 2011.

[2] It should be noted that while procedures were put in place to conduct Mistreatment Risk Assessments, an official policy (OPS-6: Mistreatment Risk Management) was only approved on September 8, 2014. An internal audit in 2014 attributed this delay in policy development and operationalization to a number of factors, including "a lack of precedence to help formulate and conduct this type of risk assessment, the wide range of stakeholders with competing interests, the ." Audit of Information Sharing with Foreign Entities by the Director of Audit, Evaluation and Ethics, July 2017, pg. 7.

[3] OCSEC letter to the Minister of National Defence: Review of CSE information sharing with Foreign Entities, March 31, 2017.

issued to the Public Safety agencies.[4]

4. Sections 24 and 27 of the 2017 MD require CSE to report annually to the Minister and to file a public copy of the report. **NSIRA observes that these requirements were fulfilled. The Minister was provided a classified report and a public copy of the report published on the CSE website.**[5]

Policies and Procedures

5. In 2018 CSE overhauled its policies and created a single, centralized policy suite named the Mission Policy Suite (MPS). There are three core policy documents which together provide the policy guidelines for the implementation of the MD:

1) The "Mission Policy Suite: Authorities, Governance and Accountability" enshrines in policy the CSE's general obligations under the 2017 MD, and requires that Mistreatment Risk Management Clauses . Additionally, the policy defines roles and responsibilities.[6]

2) The "Mission Policy Suite A" provides more specific policy guidelines for a number of MD-related issues, including but not limited to the MRA process, approval levels, as well as documentation and reporting requirements.

3) The " Standards of Operating Procedures" (SOPs) are the detailed processes that give effect to the policies set out in the Mission Policy Suite A.

Process

6. MRAs are the primary tool used to assess information sharing. information sharing that may trigger the MRA process:

Indirect information sharing. This usually involves a request by a second party to CSE SIGINT information . In these cases, the information will usually be sanitized so that the information is not attributed to CSE and the recipient cannot identify the source of the information.

7. CSE conducts two types of MRAs:

[4] Please see section on the 2017 MD in Part X of this review.
[5] https://www.cse-cst.gc.ca/en/transparency-transparence/reports-rapports/mistreatment-mauvais-traitements-2018
[6] Mission Policy Suite; Authorities, Governance and Accountability, April 2, 2019.

1) Annual MRAs: These assessments are used to exclude countries from the normal MRA process. They are updated and approved by the Chief of CSE on an annual basis. To approve an Annual MRA, the Chief must be satisfied that information sharing with the country or countries in question would not create a substantial risk of mistreatment.

2) Case-specific MRAs are conducted for each instance of proposed information sharing with foreign nations not covered by an annual MRA.

8. The case-by-case MRAs include:

- Contextual information, including information regarding the request itself, CSE's history of sharing with the foreign entity in question, and CSE's profile for the country (discussed below).
- Risk factors, including but not limited to the human rights record of the receiving entity, the type of information and its accuracy, as well as the likelihood that action such as detention will be taken on the basis of the information.
- Mitigating factors, including assurances in place, caveats, as well as any sanitization being done to minimize the extent of the information being sought or disclosed.

9. As part of this process, will will also search for reports of mistreatment by the relevant country or entity, and will .[10]

10. CSE also maintains a set of country profiles that describe the overall human rights record of the country, with attention to governance, civil liberties, detention, vulnerable populations and international relationships. Country profiles are updated

[7] Briefing Note for the Chief: Mistreatment Risk Assessment for Information Sharing with October 25, 2018.

[9] CSE briefing to NSIRA: Mistreatment Risk Management, September 10, 2019.
[10] *Ibid.*

annually or when a material change in a country's situation occurs. As noted above, the country profile forms part of the contextual information that informs each case-by-case MRA.

10. CSE currently considers countries to be Limited Risk Nations (LRNs), as they have been deemed to have "satisfactory human rights records" and to "share similar values as Canada regarding human rights and dignity".[11] Information sharing involving these nations still requires a case-by-case MRA, but the process is abbreviated and requires a lower level of approval.[12] The list of LRNs is monitored and LRN status revoked should there be a significant deterioration in a country's human rights situation.

11. The various factors described in the case-by-case MRA are analyzed collectively and a decision is made by regarding the residual risk that the information requested or shared creates a substantial risk of mistreatment despite mitigation measures. There are four outcomes: low, medium, high and substantial. The approval level for the MRA depends on the risk level:[13]

Risk Level	Risk Determination	Approval
Low (for LRNs)	Mistreatment is unlikely	Supervisor,
Low (for non-LRNs)	Mistreatment is unlikely	Manager,
Medium	Mistreatment is possible, based on theory or speculation	Director, Disclosure and Information Sharing
High	There is a substantial risk of mistreatment that can be mitigated	Senior executives, as described below
Substantial	There is a personal, present and foreseeable unmitigated risk of mistreatment	Sharing is prohibited

12. In the case of high risk information sharing, the case is typically passed to the Director General of Policy, Disclosure and Review for approval. If that individual is unsure whether the risk mitigation measures are sufficient, he or she refers the case to the Deputy Chief of Policy and Communications. If the Deputy Chief is also unsure, then he or she refers the case to the Chief of CSE.

13. **NSIRA observes that CSE has fulfilled the requirement pursuant to s. 20 the 2017 MD to "maintain policies and procedures for assessing risks associated with relationships with foreign entities".**

[11] Briefing Note for DC PolCom: Annual Review of Mission Policy Suite (MPS) Annex G: Limited Risk Nations (LRN) List, July 5, 2019.
[12] *Ibid.*
[13] Mission Policy Suite A, Chapter 4, paragraph 30.6.3(a), pg. 88.

III CASE STUDY

14. NSIRA examined the that required approval by the Chief of CSE during 2017-18.

The request to share was received by CSE on The request was flagged as urgent given the imminent nature of the threat.

15. A detailed MRA and recommendation were drafted. Of note, it included the proposed wording of the message and a description of the human rights assurances received .[14] The mistreatment risk section of the MRA included elements of CSE's country profile for the

Additionally, CSE reached out to receive more information CSE also reached out to

16. Ultimately, determined that there was a substantial risk of mistreatment, but that this risk could be mitigated by the assurances received also factored in their own numerous previous "without an indication that any such release resulted in the mistreatment of any person".[16] The case was passed to senior CSE executives, and ultimately to the Chief.

17. The Chief approved the request based on her belief that the risk of mistreatment was sufficiently mitigated. The Chief noted that the decision was based on several factors, including the strong assurances provided similar assurances received

Additionally, intended to include a caveat stating that the "information shall not be used for the mistreatment of any person within the meaning of applicable international law".[17] The decision to share the information was made on

18. As per the requirements in the MD, a notification letter was sent to the Minister of National Defence and the National Security and Intelligence Committee of

---

[14] Mistreatment Risk Assessment and Recommendation, CERRID # 40175445.
[15] This was done in order to assist in evaluating

Mistreatment Risk Assessment and Recommendation, CERRID # 40175445.
[16] *Supra* 13. Please see NSIRA's observation regarding reliance on an absence of indications of mistreatment in a specific entity found in Part V of this review.
[17] *Supra* 13.

Parliamentarians on informing them of the case and of the rationale for the final decision.[18]

19. NSIRA observes that this case was handled very promptly. CSE conducted appropriate consultations, and kept sufficiently detailed records at all levels to understand the decisions made. CSE's final decision was reasonable.

[18] CSE letter to the Minister of National Defence, the Chair of the National Security and Intelligence Committee of Parliamentarians and the Communications Security Establishment Commissioner RE: Notification under the Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities,

ANNEX E: THE ROYAL CANADIAN MOUNTED POLICE

I BACKGROUND

1. In 2011, a number of departments received Ministerial Direction on Information Sharing with Foreign Entities (the 2011 MD). The MD issued to the RCMP was limited in scope, however, as it applied only to "RCMP investigations under subsection 6(1) of the Security Offences Act, and investigations related to a terrorist offence or terrorist activity as defined in section 2 of the Criminal Code".[1] By contrast, the MD issued to CBSA, CSIS, and CSE covered all information sharing and was not limited to a specific category of activities.

2. In response to the 2011 MD, the RCMP updated its policies on information sharing and created a new centralized system of governance and oversight housed within the Federal Policing and Criminal Operations (FPCO) branch at RCMP headquarters. FPCO was at the time responsible for national security criminal investigations, including information sharing with foreign entities. The RCMP also created the Foreign Information Risk Advisory Committee (FIRAC), which was tasked with assessing the potential risk of mistreatment associated with information sharing related to the national security program.[2] RCMP investigators referred cases to FIRAC on an "as needed" basis when they felt that the information sharing may lead to the mistreatment of an individual, when the implicated foreign entity's record in complying with caveats and assurances was poor, or when the use of caveats and assurances was unlikely to mitigate the risk of mistreatment.[3]

II THE 2017 MINISTERIAL DIRECTION

3. On September 25, 2017, the RCMP received new Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities (the 2017 MD). This time, the MD received by the RCMP was effectively identical to that issued to other departments, and was no longer limited in scope to national security investigations. As a result, the MD applied to all investigations involving information sharing with foreign entities, including narcotics and child sexual exploitation cases as well as national security. In response to the expanded scope of the 2017 MD, the RCMP contemplated alternative

---

[1] Ministerial Direction to the Royal Canadian Mounted Police: Information Sharing with Foreign Entities, 2011.
[2] Annual Report, Ministerial Direction to the RCMP: Avoiding Complicity in Mistreatment by Foreign Entities. September 25, 2017-September 25, 2018.
[3] *Ibid.*

models to implement the MD, but ultimately decided that its existing FIRAC model best addressed the RCMP's needs.[4]

4. Sections 24 and 27 of the 2017 MD require the RCMP to report annually to the Minister on the implementation of the MD and to file a public copy of the report. **NSIRA observes that these requirements were fulfilled. The Minister was provided a classified report and a public copy of the report was published on the RCMP website**.[5]

Policies and Procedures

5. As noted above, the 2017 MD significantly expanded the scope of RCMP information sharing subject to MD. This change triggered extensive work to update the RCMP's policies and procedures to conform to the new requirements. This work is ongoing.

6. The RCMP Operational Manual (OM) contains the two main policies governing information sharing:

1) OM Chapter 12.3: Sharing, Handling and Release/Dissemination of Information. This chapter contains the procedures for sharing information with domestic departments, foreign entities, record-keeping requirements, mandatory caveats, and protocols for interactions with countries with questionable human rights records.

2) OM Chapter 44.1: Sharing Information with Foreign Law Enforcement. This chapter contains a clause stating that information sharing must be done in accordance with applicable treaties, legislation and Ministerial Directives.[6] The chapter outlines specific roles and responsibilities such as the operational chain for information sharing.

7. These policies are consistent with the 2011 MD, but have not yet been updated to reflect the 2017 MD. While the RCMP has developed, and put into practice, new processes that give effect to the 2017 MD, these processes have not been integrated into the overarching Operational Manual. The RCMP has informed NSIRA, however, that it is in the process of updating its Operational Manual to reflect its post-2017 practices.[7] **NSIRA observes that once integrated, the RCMP will have fully**

---

[4] RCMP Implementation of the Avoiding Complicity in Mistreatment by Foreign Entities Act: Briefing to NSIRA Review Direction, October 3, 2019.
[5] http://www.rcmp-grc.gc.ca/en/rcmp-annual-public-report-the-ministerial-direction-avoiding-complicity-mistreatment
[6] Chapter 44.1, Section 1.3: "The sharing of information will be managed on a case-by-case basis in compliance with the Canadian Charter of Rights and Freedoms, applicable treaties and legislation, in accordance with Ministerial Directives, Policy, and officially sanctioned Memorandum of Understanding (MOUs) or agreements."
[7] RCMP Briefing to NSIRA, October 3, 2019. This shortcoming was also noted internally in the "Federal Policing, Foreign Information Risk Advisory Committee: One Year Review", Federal Policing Strategic Direction Branch, August 30, 2019, pg. 12. This internal review is discussed below.

implemented s. 20 of the 2017 MD, which requires the RCMP to "maintain internal policies and procedures for assessing the risks associated with relationships with foreign entities".

The Law Enforcement Assessment Group (LEAG)

8. Following receipt of the 2017 MD, the RCMP established a new Law Enforcement Assessment Group (LEAG). LEAG has a detailed Terms of Reference that outlines its membership as well as roles and responsibilities.[8] LEAG's primary task is to assess foreign countries and law enforcement entities with regard to the risk of mistreatment. In its assessments, LEAG considers a number of factors, including the human rights record of the country, specific foreign entities' engagement in human rights abuses,[9] local law enforcement's history of respecting caveats, as well as country-specific risks to individual safety related to political views, religion, ethnicity, sexual orientation, and so on. LEAG thus "plays an integral role in informing FIRAC's decision on whether to share information with foreign law enforcement entities".[10]

9. LEAG's reports place countries into one of three categories:

Colour	Risk Level	Approval
Green	Low risk of mistreatment	Information may be shared [11]
Yellow	Medium/possible risk of mistreatment	If certain factors are present, case must be referred to FIRAC for decision
Red	High risk of mistreatment	Case must be referred to FIRAC for decision

10. At present, the RCMP has categorized 146 approved country profiles, of which 20 are high risk, 69 are medium risk, and 57 are low risk. 51 country assessments remain outstanding.[12] LEAG currently intends to update its profiles every two years, although LEAG will update some reports more frequently based on operational requirements.[13] To date, 40 countries have been assessed as being a high priority for periodic updates due to the volume of information sharing conducted.

---

[8] LEAG's membership includes representatives from Federal and International Special Services, INTERPOL (Ottawa Bureau), Federal Policing Criminal Operations, the National Intelligence Coordination Centre, Federal Policing Support Services, Federal Policing Intelligence and International Planning, Federal Policing National Security, and the Canadian Police Centre for Missing and Exploited Children's Behavioural Sciences Branch. See the Terms of Reference: Law Enforcement Assessment Group.
[9] Although noted in the ToR, LEAG has informed us that this information is not standard but is included when available. See the RCMP Briefing to NSIRA, October 3, 2019.
[10] Terms of Reference: Law Enforcement Assessment Group.
[11] Such information sharing is still subject to other Canadian law, including the *Charter* and the *Privacy Act*, as well as the RCMP's information sharing MoUs. See the RCMP Implementation of the Avoiding Complicity in Mistreatment by Foreign Entities Act: Briefing to NSIRA Review Direction, October 3, 2019.
[12] "Foreign Information Sharing Country Assessments", LEAG document dated September 6, 2019.
[13] RCMP Briefing to NSIRA, October 3, 2019.

11. LEAG's country reports include both open source and classified information. Each report follows a set template, which includes a country overview, a list of law enforcement entities in the country, the key human rights considerations, the results of other Government of Canada information sharing assessments, and the results of foreign information sharing country assessments.[14] When available, country profiles include input from RCMP liaison officers posted abroad. **NSIRA observes that the key human rights considerations sections of the country reports are detailed and address wide-ranging human rights concerns.[15]**

The Foreign Information Risk Advisory Committee (FIRAC)

12. FIRAC is the advisory body tasked with assessing information sharing cases where there is a substantial risk of mistreatment. FIRAC reviews each such case to determine whether this risk can be mitigated, and discusses the best mitigation strategies to employ. If FIRAC cannot determine whether the substantial risk can be mitigated, it refers the decision to a more senior level of approval.[16] FIRAC also "serves as a forum to assess and provide recommendations to management as to when to notify Global Affairs Canada (GAC) that an operation or activity may represent a risk to foreign policy".[17]

13. Following the issuance of the 2017 MD, FIRAC membership was expanded to reflect the new business lines involved in information sharing newly subject to MD.[18] Nonetheless, the FIRAC Chair remains a senior national security officer, currently the Director General of Federal Policing National Security Operations. The Chair is supported by a small secretariat.[19] While in theory FIRAC meets on an "as needed" basis, in practice the sheer volume of information sharing requests means that it normally meets at least once a week.[20]

14. It is worth emphasizing that FIRAC does not merely consider cases where an RCMP officer is *unsure* whether a substantial risk can be mitigated, but rather considers all cases where a substantial risk has been identified. As a result, all decisions regarding the sufficiency of mitigating measures are made by a well-informed committee

---

[14] LEAG Country Risk Profile Template.
[15] Key human rights considerations incorporated into the country profile template include an analysis of extrajudicial or arbitrary torture or killing; arrests; detention and solitary confinement; the death penalty; systemic abuse; specific groups that may be subject to human rights abuses (women, LGBTQ, human rights lawyers, activists, specific forms of criminality); recent changes to human rights laws; and any other relevant information that could assist in assessing the potential risk of mistreatment associated with the country. *Ref: Ibid.*
[16] Terms of Reference: Foreign Information Risk Advisory Committee.
[17] *Ibid.*
[18] Current FIRAC membership includes the Director General of Federal Policing National Security (Chair); the Director, Federal Policing National Security (Co-Chair); the Director General, Contract and Indigenous Policing; the Director General, Federal Policing Intelligence and International Policing; the Director, Strategic Policy, Federal Policing Strategic Direction; the Manager, External Review and Compliance (record-keeper), Federal Policing Strategic Direction. Occasionally the investigators involved in the case will be present to address specific concerns.
[19] *Supra* 13, 16.
[20] *Supra* 4, 13.

rather than a single officer, who may have a vested interest in sharing the information in question. As such, **NSIRA observes that FIRAC's broad role and independence significantly strengthen the RCMP's information sharing process**.

Process

15. If an RCMP officer identified a need and wishes to share information with a foreign entity, they must follow a set process:[21]

A. The officer must first consult a specific RCMP intranet website created by LEAG. The site lists countries by colour. If the officer finds that the country in question is "green", he or she may proceed to share the information. If the country is "red" – or "yellow" *and* the circumstances of the proposed sharing match *any* of the case-specific factors and considerations listed – then the case must be referred to FIRAC. For example:[22]

NSIRA observes that this system results in a clear and streamlined risk assessment process for requests. Under this system, RCMP officers – who

[21] Requests for information overseas go through the posted liaison officer who then process the requests via headquarters. *Supra* 13.
[22] Foreign Information Sharing Country Assessments. Received on December 19, 2019.

may lack expertise regarding human rights concerns in specific countries and who have a personal stake in the outcome of operations – are not required to make subjective judgements regarding the probability of mistreatment stemming from information sharing.

B. If a FIRAC is required, the officer completes a standard form which must be approved by the relevant Criminal Operations (CROPS) Officer or other approving officer.[23] The form includes a summary of the information to be shared, the kind of sharing (request, disclosure or use), the operational context, the risks of sharing information, the investigative value of the information, possible mitigation strategies, and – where applicable – the actual information to be disclosed or used.[24]

C. Once approved, the form is sent to the Director General (DG) responsible for the relevant program at RCMP headquarters for approval. Following approval, the DG submits the form to the FIRAC secretariat.

D. The FIRAC secretariat compiles a briefing package that includes the officer's form, the country profile from LEAG, and any supporting documentation submitted by the DG. The briefing package is distributed to FIRAC members ahead of the meeting.

E. A FIRAC meeting is convened and the request is considered along with possible mitigation strategies. While the final decision regarding FIRAC's recommendation rests with the Chair, in the vast majority of cases the decision is unanimous. Dissenting opinions are recorded in the Record of Decision (RoD). Once FIRAC has noted its recommendation, the RoD and an accompanying briefing note are sent to the Assistant Commissioner for final determination.

F. In cases where FIRAC cannot determine whether a substantial risk of mistreatment can be mitigated, the responsible Assistant Commissioner will provide the RoD to the Deputy Commissioner in order to obtain the Commissioner's decision.

16. FIRAC's RoDs follow a standard template. **NSIRA observes that while the RoD provides details of the proposed sharing and mitigation measures, there would also be value in keeping minutes of FIRAC meetings. These would shed additional light on the considerations that informed FIRAC's recommendation.**[25]

---

[23] Foreign Information Risk Advisory Committee (FIRAC) Process Chart, January 7, 2019. RCMP Implementation of the Avoiding Complicity in Mistreatment by Foreign Entities Act: Briefing to NSIRA Review Division, October 3, 2019.
[24] Instructions: Outline of Investigative Requirements and Operational Context: Foreign Information Risk Advisory Committee, Form 6517e (2019-2).
[25] This issue was also noted internally by the RCMP in the Federal Policing, Foreign Information Risk Advisory Committee: One Year Review, Federal Policing Strategic Direction Branch, August 30, 2019, pg. 11.

Internal Review

17. In June 2019, the RCMP conducted an internal review of the framework and policies in place for FIRAC and LEAG. The review identified various shortcomings regarding processes, policies, training and resourcing. NSIRA was provided with a copy of the review, even though the review had not yet received final approval. Based on the draft provided, **NSIRA observes that the review was thorough and frank in identifying areas in need of improvement.**

18. NSIRA observes that periodic internal reviews to identify gaps and areas for development, such as the one undertaken by the RCMP, should be considered a best practice for all departments.

III CASE STUDY

19. For its case study, NSIRA chose an ongoing investigation into two Canadians who are alleged to have travelled order to participate in the activities of a listed terrorist group. In this instance, the RCMP sought to share the names of potential witnesses in the in order to locate and speak to these witnesses.

20. The case originated from the Federal Policing National Security Branch. The request for a FIRAC determination was submitted on April 26, 2018. LEAG had assessed being a medium risk (yellow) country. In this case, the nature of the proposed disclosure of information necessitated a FIRAC meeting.[26]

21. LEAG's risk profile was exceptionally detailed, and contained extensive information regarding the country's human rights record and partner agency concerns. It included assessments of individual law enforcement entities in the country and discussed the possibility of the dissemination of RCMP information amongst these agencies. The country risk profile was current as of April 19, 2018.[27]

22. A FIRAC was held on April 27, 2018, to discuss the request. FIRAC found that there was a substantial risk of mistreatment should the information be shared and that the proposed mitigation measures were unlikely to mitigate the risk. Accordingly, FIRAC recommended that the information sharing not proceed. FIRAC also noted that renewed assurances should be sought by the RCMP liaison officer , if obtained,

---

[26] Foreign Information Risk Advisory Committee: Outline of Investigative Requirements and Operational Context, Cover Sheet, April 26, 2018.
[27] Foreign Information Sharing Assessment of Risk; Country Risk Profile: Medium, RCMP Liaison Office: April 19, 2018.

the request to share information could be resubmitted to FIRAC for further deliberation.[28]

23. The Assistant Commissioner concurred with the recommendation and provided official approval on May 1, 2018.[29] **NSIRA observes that this case was handled promptly and appropriate consultations were conducted. Internal procedures were followed, a case-specific assessment was conducted, and the recommendation made by FIRAC was reasonable.**

[28] Foreign Information Risk Advisory Committee: Record of Decision, April 27, 2018.
[29] Briefing Note to the Assistant Commissioner, Foreign Information Risk Advisory Committee: Recommendation to Not Exchange Information, submitted April 30, 2018, approved May 1, 2018.

ANNEX F: THE CANADIAN SECURITY INTELLIGENCE SERVICE

I BACKGROUND

1. The Canadian Security Intelligence Service (CSIS) was one of the first Government of Canada departments to receive Ministerial Direction (MD) regarding information sharing with foreign entities.[1] In May 2009, CSIS received MD on Information Sharing with Foreign Agencies.[2] This MD focused on the importance of information sharing for the effective execution of CSIS's mandate and reiterated CSIS's authority to enter into information sharing arrangements even with countries "generally recognized as having poor human rights records".[3] Nonetheless, the MD noted its opposition to torture and directed CSIS to not knowingly rely on information derived from the use of torture and to use appropriate measures to identify such information. The MD placed few parameters on the disclosure and requesting of information potentially resulting in torture beyond exhorting CSIS to take "reasonable measures" not to condone or promote torture through the use of assurances.[4]

2. In July 2011, the MD was replaced by a new MD on Information Sharing with Foreign Entities (the 2011 MD).[5] The 2011 MD placed new parameters on the use of information derived from mistreatment, as well as the disclosure and requesting of information that may lead to a substantial risk of mistreatment. In response, CSIS issued the DDO Directive on Information Sharing with Foreign Entities.[6] The Directive provided wide-ranging guidance on the process for information sharing with foreign entities and created a new Information Sharing Evaluation Committee (ISEC), whose role is described in detail below.[7]

---

[1] Although the Integrated Terrorism Assessment Centre (ITAC) functions as a resource for the entire security and intelligence community, it forms part of CSIS from the standpoint of corporate accountability. As such, ITAC must comply with CSIS's framework for information sharing and mistreatment. Although NSIRA did not review ITAC specifically, ITAC informed NSIRA that it does have a framework for avoiding complicity in mistreatment by foreign entities, and that it is particularly cautious in using reporting derived from detainees.
[2] Ministerial Direction to the Director of the Canadian Security Intelligence Service: Information Sharing with Foreign Agencies, May 2009.
[3] *Ibid.*
[4] *Supra* 2.
[5] Ministerial Direction on Information Sharing with Foreign Entities, July 28, 2011.
[6] DDO Directive on Information Sharing with Foreign Entities, August 24, 2011.
[7] A review of this process was conducted in 2015 by NSIRA's predecessor organization, SIRC. SIRC Review 2015-003, Review of Ministerial Direction and CSIS Directives on Information Sharing, November 18, 2015.

II THE 2017 MINISTERIAL DIRECTION

3. On September 25, 2017, the 2011 MD was replaced by the new MD on Avoiding Complicity in Mistreatment by Foreign Entities (the 2017 MD). The 2017 MD brought significant changes. A notable addition was a requirement that CSIS provide the Minister with an annual report on its implementation of the MD and that a copy of the report be made public. **NSIRA observes that these requirements were fulfilled. The Minister was Provided a classified report and a public copy of the report published as part of the CSIS annual report.**[8]

Policies and Procedures

4. CSIS information sharing with foreign entities are governed by formal arrangements established pursuant to s. 17 of the *CSIS Act*. In the absence of a s. 17 arrangement, information can only be shared with ministerial approval or – in exigent circumstances – by the Director.[9] Currently, CSIS has foreign relationships in countries.[10]

5. The primary policy instrument implementing the 2017 MD is the DDO Directive on Avoiding Complicity in Mistreatment by Foreign Entities, which was issued in September 2017 just days following the issuance of the 2017 MD.[11] This directive outlines the process to be followed when sharing or providing information as well as related requirements such as record keeping. Additionally, the directive includes the terms of reference for the Information Sharing Evaluation Committee (ISEC). ISEC serves as an advisory body whose primary function is to review cases where there is uncertainty regarding whether a substantial risk of mistreatment can be mitigated.

Restriction Levels

6. Section 22 of the 2017 MD required CSIS to restrict its foreign information sharing arrangements if "it is assessed by CSIS that a foreign entity is engaging in, or contributing to, mistreatment". In response, in April 2018 CSIS rolled out a new system of restriction levels that categorizes foreign entities according to their level of risk. **NSIRA observes that the DDO Directive issued in 2017 remained in place alongside the new systems of restriction levels, but the DDO Directive's processes and decision charts were not updated to take into account the new restriction levels.** As a result, CSIS employees must interpret several documents in order to understand the process they must follow.

---

[8] https://www.canada.ca/en/security-intelligence-service/corporate/publications/2018-public-report.html

[9] OPS-602: Disclosure of Security Information or Intelligence, 2011-11-28. Ministerial Direction on Operations and Accountability, 2015.

[10] CSIS Arrangements with Foreign Governments and Institutions, January 2020.

[11] Memorandum: DDO Directive on Avoiding Complicity in Mistreatment by Foreign Entities, September 28, 2017.

7. CSIS has informed NSIRA that it is overhauling its current policies and procedures with the goal of facilitating information sharing. The anticipated result of these changes will be a greater volume of information sharing with foreign entities.[12] New policy and process documents should provide integrated and streamlined guidance.

8. CSIS's information sharing restriction levels are described below:[13]

Restriction	Description	Authority to Share
Level 1	Full restriction due to extremely serious human rights concerns or foreign policy requirements	Prohibited – no information sharing
Level 2	Some restriction due to serious human rights concerns	Non-personal information deemed not to present a potential risk of mistreatment may be shared Decisions to share information pertaining to specific individuals are referred to ISEC
Level 3	Some restriction due to serious human rights concerns but where ability to mitigate the risk of mistreatment through caveats and assurances is established	Non-personal information deemed not to present a potential risk of mistreatment may be shared Decisions to share information pertaining to specific individuals are referred to the CSIS program Director General (DG) who determines whether there is a substantial risk of mistreatment that can be mitigated; if the DG cannot make this determination, the decision is referred to ISEC

9. Each country's restriction level is determined by information regarding the country's overall human rights record, as well as information regarding the conduct of the relevant foreign entities in each country. This includes information from:[14]

- Open sources such as Amnesty International and Human Rights Watch;

[12] CSIS briefing to NSIRA, September 12, 2019.
[13] Memorandum to the Minister: Restrictions imposed on CSIS Act s. 17(1)(b) Foreign Arrangements, Annex 1: Restrictions, April 3, 2018.
[14] *Supra* 12.

- Other Government of Canada departments such as Global Affairs Canada;
- CSIS stations abroad; and
- Foreign intelligence partners that have experience dealing with the foreign entities in question.

10. Currently, CSIS has placed some level of restriction on information sharing with entities in of the countries with which they have s. 17 arrangements.[15] As noted above, a key difference between levels 2 and 3 is CSIS's confidence that the risk of mistreatment can be mitigated by means of caveats and assurances. NSIRA was informed, however, that the seriousness and frequency of the mistreatment allegations are also considered.[16]

11. In examining CSIS's restriction levels, NSIRA considered two countries,

13. In discussions, NSIRA was reminded that final decisions regarding restriction levels lie with CSIS executives.

Such decisions, alongside the other discrepancies noted above, give the impression that

[15] *Supra* 12.
[16] *Supra* 12.
[17] *CSIS Act* s. 17(1)(b) Foreign Arrangement –
[18] *Supra* 12.

CSIS is prioritizing strategic partnerships over an objective assessment of the potential for mistreatment stemming from information sharing.

Process

14. CSIS's information sharing process can be summarized as follows:

A. An desk needing to disclose or request information with a foreign entity determines whether:[19]

i. the information pertains to an individual in detention abroad;

ii. the information could result in a negative action against an individual (such as detention); and/or

iii. there are other indications of a potential for mistreatment.[20]

If none of the criteria above and no restriction level is present, then the desk may disclose or request the information. Otherwise the case must be referred to the Deputy Director General of DDG).

B. The DDG assesses the proposed information sharing and conducts the next stage or triaging where the following factors are taken into consideration:

i. If the information involves a level 1 restricted entity, no information may be requested or shared.

ii. If there is a potential risk of mistreatment and the country is a level 2 restricted entity, the DDG refers the case to ISEC via his or her DG.

iii. If there is potential risk of mistreatment and the restriction level is 3, then the case is referred to the DG of the relevant branch, who determines whether the risk can be mitigated so that the residual risk is not substantial. If the DG finds that the risk can be mitigated, then the information is shared with the appropriate caveats and assurances. If the DG is unsure or wishes to receive additional guidance, however, the case is referred to ISEC.[21]

iv. If, for an entity that has no restriction level, there is a potential risk of mistreatment that can be mitigated so that the residual risk of mistreatment is less than substantial, the information can be disclosed or requested, with appropriate caveats and assurances.

---

[19] *Supra* 11.
[20] *Supra* 11.
[21] *Supra* 11, 13.

C. Once referred to ISEC, the ISEC secretariat circulates a case brief prepared by the requesting branch. The brief includes a summary of the case including the operational rationale for the request, a copy of the proposed correspondence, a summary of the human rights record of the foreign entity, documentation related to CSIS's s. 17 arrangement with the entity, as well as any assurances or other mitigating factors.

Information Sharing Evaluation Committee

15. ISEC comprises a number of Directors General from relevant CSIS branches, including the DG of the branch that is involved in the proposed information sharing or use. ISEC also includes a General Counsel from CSIS's Departmental Legal Services[22] (DLS) and a manager from Global Affairs Canada. ISEC convenes on an as-needed basis to consider a specific case. ISEC operates on the basis of consensus, albeit with counsel serving only in an advisory capacity.[23]

16. ISEC may come to one of three conclusions when disclosing or requesting information:

1) The proposed measures are sufficient to mitigate the substantial risk of mistreatment, and accordingly the information may be shared.

2) The substantial risk of mistreatment cannot be mitigated and accordingly the information may not be shared.

3) There remains uncertainty as to whether the substantial risk of mistreatment has been sufficiently mitigated by the proposed mitigation measures (such as caveats and assurances), and accordingly the case should be referred to the Director of CSIS for decision.

17. ISEC maintains extensive records. This includes documentation of the requesting branch's summary of the case, minutes of the discussion, as well as a description of the importance of the information to be shared.

[22] CSIS Departmental Legal Services (DLS) comprises lawyers from the Department of Justice's National Security Litigation and Advisory Group (NSLAG).
[23] Memorandum: DDO Directive on Avoiding Complicity in Mistreatment by Foreign Entities, Annex 3: Information Sharing Evaluation Committee, September 28, 2017.

III CASE STUDY

18. As its case study, NSIRA chose a situation involving threat-to-life information emanating from an investigation of an individual in
for several years.[24]

30. This case raises several concerns. **NSIRA observes that while the case was described as involving a threat to life, it was not handled with the urgency of a genuine threat to life case.** If the goal of the proposed sharing of information was to protect life, CSIS acted too slowly. ISEC did not convene for eight days after the case was referred, and it ultimately took CSIS over two months to make a definitive decision

---

regarding the proposal,

31.

NSIRA's predecessor organization, the Security Intelligence Review Committee (SIRC), recently noted ISEC's tendency to avoid clear but unpopular decisions not to share information by referring matters to the Director.[48]

32. Finally, **NSIRA observes that CSIS's record-keeping in this case was slow and incomplete**, as the August 14, 2019, draft minutes of the June 27, 2019, ISEC meeting did not reflect the current status of the case.

[48] SIRC: Certification of the Director's Annual Report to the Minister of Public Safety (SIRC study 2018-07, Annex B, March 21, 2019).

ANNEX G: THE DEPARTMENT OF NATIONAL DEFENCE AND THE CANADIAN ARMED FORCES

I BACKGROUND

1. In 2011, the Government of Canada issued Ministerial Direction on Information Sharing with Foreign Entities (the 2011 MD) to a number of departments, including CSIS, CSE, CBSA, and the RCMP.[1] The Department of Defence (DND) and the Canadian Armed Forces (CAF) did not receive the 2011 MD, however. NSIRA was informed that there had been plans to issue the 2011 MD to DND/CAF, but that the letter was never signed by the Minister.[2]

2. Regardless, DND/CAF had already issued internal guidance regarding information sharing. On June 14, 2010, the Chief of Defence Intelligence (CDI) issued the "Functional Directive on Intelligence and Intelligence-Derived Information Sharing with External Entities" (2010 CDI FD). The policy objective of this directive was to "establish direction, institute procedures, direct the accountability, and establish oversight mechanisms for the sharing of defence intelligence and intelligence-derived information with external entities".[3]

3. The 2010 CDI FD defined the roles of:

- The Release and Disclosure Coordination Office (RDCO) – part of the Canadian Forces Intelligence Command (CFINTCOM) – responsible for managing and monitoring the release and disclosure process;[4]

- Release and Disclosure Officers (RDOs) who are designated, trained and certified officers responsible for approving or declining requests to share intelligence and intelligence-derived information with external entities; and

- Release and Disclosure Authorities (RDAs) who are designated, trained and certified persons responsible for implementing the CDI FD as well as nominating RDOs and providing them with guidance on the sharing of defence intelligence. In addition to their responsibilities, RDAs can fulfill the same functions as RDOs.

---

[1] Ministerial Direction: Information Sharing with Foreign Entities, 2011.
[2] Briefing to the National Security and Intelligence Review Agency, September 20, 2019.
[3] CDI Functional Directive on Intelligence and Intelligence-Derived Information Sharing with External Entities, June 14, 2010.
[4] DND/CAF has clear distinctions between release and disclosure. Release is the "transfer of intelligence-derived information via electronic or any other means, resulting in the ability of the recipient to manipulate, reproduce or further disseminate the original information" while disclosure is the "transfer of intelligence-derived information by permitting the recipient to view or hear intelligence-derived information without any physical transfer of information". *Ibid*.

4. Many of these roles and responsibilities have continued to the present day.[5] DND/CAF released further Functional Directives from 2010 to 2017 that built on and modified the framework first established in 2010. Some pertained to information sharing with specific countries, while others focused on information sharing in the context of specific operations.[6]

5. Though DND/CAF's framework was comparable in many ways to the 2011 MD, the threshold for the sharing of information in the 2011 MD was somewhat different than the threshold set out by DND/CAF. The CDI FD stipulated that "before sharing intelligence or intelligence-derived information with an external entity, RDAs and RDOs shall determine whether, as a result of such sharing, there is a reasonable likelihood that the recipient will engage in torture or use the intelligence or intelligence-derived information in violation of Canada's obligations. Where it is more likely than not there will be mistreatment or torture, RDAs and RDOs shall seek direction from RDCO prior to sharing. Where there is 'substantial risk' of personal, present and foreseeable risk of mistreatment or torture, RDAs and RDOs cannot share intelligence or intelligence-derived information".[7] The 2010 CDI FD did not define the term "substantial risk".

6. By contrast, the 2011 MD defined "substantial risk", and also noted that "the 'more likely than not' test should not be applied rigidly because in some cases, particularly where the risk is of severe harm, the 'substantial risk' standard may be satisfied at a lower level of probability".[8]

II THE 2017 MINISTERIAL DIRECTION

7. On November 24, 2017, DND/CAF received the Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities. In 2017, the same direction was also issued to GAC and the departments that had received the 2011 MD.

8. Sections 23 and 25 of the 2017 MD require DND/CAF to report annually to the Minister on the implementation of the MD and to file a public copy of the report. **NSIRA observes that DND/CAF fulfilled the requirement to report to the Minister. An unclassified version of the report has not yet been publicly released.**[9]

---

[5] *Supra* 3, s. 1.8.
[6] Additional Functional Directives issued include the CDI FD on Intelligence
: CDI FD on the Release and Disclosure
; CDI FD
CDI FD Briefing to the National Security and Intelligence Review Agency, September 20, 2019.
[7] *Supra* 3, s. 2.5.
[8] *Supra* 1, s. 2.
[9] NSIRA has been provided with the unclassified version of the report and was informed that it will be published shortly. DND/CAF e-mail to NSIRA, re: MD Review - Unclassified report DND/CAF, January 15, 2020.

Policies and Procedures

9. Following receipt of the 2017 MD, DND/CAF issued two additional directives:

1) The "Deputy Minister of National Defence and Chief of the Defence Staff Directive on the Disclosure, Request and Use of Information: Avoiding Complicity in Mistreatment by Foreign Entities". Issued in April 2018, the directive promulgated the requirements set out in the 2017 MD.[10]

2) The "CDI Interim Functional Directive: Information Sharing with Certain Foreign States and their Entities". Also issued in April 2018, the Directive went into more detail than the higher level Deputy Minister (DM)/Chief of the Defence Staff (CDS) Directive. The Directive provided a definition of substantial risk identical to that in the 2017 MD, outlined assessment requirements pursuant to the 2017 MD, outlined categories of mitigation measures, defined the roles and responsibilities of various parties, and provided a list of "Low Risk Countries". Information sharing with these countries would still require case-by-case assessment, but in an abbreviated form.[11]

10. DND/CAF is currently in the process of overhauling its processes in order to fully implement the 2018 CDI Functional Directive. DND/CAF has intensified its training for individuals seeking RDO designation by extending the training from one to two days and offering the training to a greater number of individuals.[12]

11. For the time being, DND/CAF relies on classified reporting from its own sources, other government departments, allies, as well as unclassified open source reporting, to maintain the list of Low Risk Countries set out in the CDI Functional Directive. In future, DND/CAF intends to maintain its own comprehensive set of Country Human Rights Profiles that assess the risk of mistreatment at the country level.[13]

12. Within its operational commands, DND/CAF currently undertakes an assessment process prior to establishing information sharing arrangements with partners in medium and high risk countries. This process examines a range of risks, including those associated with information sharing. The process is not standardized, however. DND/CAF is developing new standardized tools to formalize and improve the current process.[14] **NSIRA therefore observes that DND/CAF has not fully fulfilled the**

---

[10] The DM/CDS Directive on the Disclosure, Request and Use of Information: Avoiding Complicity in Mistreatment by Foreign Entities issued on April 2018. The policy includes a detailed process chart.
[11] Chief of Defence Intelligence: Interim Functional Directive: Information Sharing with Certain Foreign States and Their Entities: Annex A: Foreign States with Low Risk of Engaging in Mistreatment. April 20, 2018.
[12] The 2017-2018 Classified Annual Report to the Minister on Avoiding Complicity in Mistreatment by Foreign Entities noted that "over 100 CAF members and DND employees from CFINTCOM, CJOC, CANSOFCOM and other L1 organisations have been certified as RDOs since the program was last updated in November 2017". NSIRA has been informed that an additional 220 persons have been certified since the report (December 2018 to December 2019).
[13] E-mail responses to NSIRA, MD on Avoiding Complicity in Mistreatment by Foreign Entities (NSIRA 2019-02), October 11, 2019.
[14] *Ibid.*

requirement, in s. 19 of the 2017 MD, to maintain internal policies for assessing the risks associated with relationships with foreign entities. DND/CAF intends to address this gap in the near future, however, by implementing the improvements described above.

Defence Information Sharing Committee (DISAC)

13. The 2017 DM/CDS Directive created the Defence Information Sharing Assessment Committee (DISAC). DISAC's primary objective is to act as an advisory committee for the DM and CDS in support of their decision-making regarding issues pertaining to the 2017 MD.[15] Cases are referred to DISAC when there is uncertainty as to whether the risk of substantial mistreatment that would result from information sharing can be mitigated.[16] DISAC completes a full risk assessment that includes findings and recommendations. DISAC then advises the DM and CDS of their proposed course of action for final decision.[17]

Defense Information Sharing Working Group (DISWG)

14. In 2019, DND/CAF stood up the Defense Information Sharing Working Group (DISWG) to act as an advisory body to DISAC. In practice, DISWG is a senior-level (Director and Colonel) triaging group that provides advice on issues that relate to the MD.[18] DISWG provides advice to operational commanders on matters related to the risk of mistreatment and mitigation measures. Furthermore, DISWG discusses general issues pertaining to the implementation of the MD and specific operations that engage the MD. DISWG maintains records of their meetings. Senior DND/CAF officials, up to and including the CDS and DM, are routinely briefed on the outcomes of DISWG discussions.[19] DISWG meets monthly, or more frequently if required.[20]

Process

15. DND/CAF differs from most departments in that most of its information sharing will take place in theatre in the context of specific operations. Nonetheless, DND/CAF has set out a process that applies regardless of whether the proposed information sharing would be conducted via headquarters or in an operational theatre:[21]

---

[15] DISAC includes members from ADM (Policy), Strategic Joint Staff (SJS), the Judge Advocate General (JAG), Canadian Forces Legal Advisor (CFLA), operational commands and other consultative stakeholders as required. DM/CDS Directive on the Disclosure, Request and Use of Information: Avoiding Complicity in Mistreatment by Foreign Entities, April 2018.
[16] *Supra* 10.
[17] *Supra* 10, Annex 2 to Tab A.
[18] Members include (but are not limited to) legal advisors from both DOJ and JAG, ADM Policy, directors from the Canadian Joint Operations Command, Canadian Special Operations Command and the Canadian Forces Intelligence Command.
[19] Briefing to NSIRA, September 20, 2019.
[20] DISWG also meets monthly or as required to discuss intelligence reporting or non-governmental reports related to mistreatment.
[21] *Supra* 10, 19.

A. An RDA (at headquarters) or an RDO (located in theatre) – officers embedded in their respective chains of command – receives a request to disclose or request information. If the officer determines that there is no substantial risk of mistreatment, the information can be shared, in accordance with any applicable MOUs, arrangements, policies and procedures. The decision to share information is recorded by the RDO. **NSIRA observes that most records are not submitted to the RDCO for central record-keeping. There is also no mechanism at the RDCO to track and review records for compliance.**

B. If an RDO determines that there is a substantial risk of mistreatment or is unsure, the RDO elevates the case through their chain of command to the task force commander in theatre and onwards to the Level One (L1) Operational Commander (a senior general or equivalent in Ottawa). Concurrently, the RDO elevates the matter to the RDA and/or RDCO for transmission to DISWG. DND/CAF informed NSIRA that, in practice, RDOs and RDAs are trained to elevate cases that involve any unusual risks or circumstances well before the threshold of "substantial risk" has been met.

C. The case is then elevated.

    a. The RDA or RDCO convenes a DISWG meeting to discuss the information sharing request.

    b. The L1 Operational Commander, on the advice of DISWG and in consultation with an RDA and legal and policy advisors, can decide whether the proposed information sharing meets the threshold of substantial risk and the mitigation measures are sufficient, or can send the matter to DISAC.

D. DISWG is convened and considers the case. The RDCO then provides a RoD containing advice, which may include a proposed course of action, to:

    a. The relevant L1 Operational Commander. If the commander is then of the view that the proposed information sharing is permissible under the MD, he or she may authorize the disclosure or request. The commander also provides an update to the DM and CDS. If the commander is still unsure as to whether the substantial risk of mistreatment can be mitigated, DISAC is convened.

    b. The Director of Staff for the Strategic Joint Staff and the Assistant Deputy Minister for Policy. These individuals evaluate the RoD and convey their concerns and reservations, if any, directly to the CDS and DM.

E. This parallel process is meant to ensure that the most sensitive decisions do not rest exclusively with a single commander.

F. If convened, DISAC makes a recommendation to the DM and CDS. The CDS will then provide direction to the relevant commander regarding the way forward.[22]

III CASE STUDY

16. To date, DISWG has not encountered any cases that it deemed to require referral to DISAC. For this reason, NSIRA did not review a specific instance of information sharing, but rather examined DISWG meeting RoDs to gain insight into DND/CAF information sharing practices related to the 2017 MD. NSIRA found that the majority of these RoDs related to Operation IMPACT. DND/CAF's mandate for this operation includes supporting the global coalition to defeat Daesh in Iraq and Syria, as well as working with partners to set conditions for stability and security.[23] In doing so, DND/CAF must ensure compliance with the 2017 MD while operating in an extremely hostile environment where threats to Canadian and allied personnel arise constantly.

17. Iraq's long history of institutionalized disregard for human rights has been widely documented. The 2019 Human Rights Watch report stated that "under the guise of fighting terror, Iraqi forces arbitrarily detained, ill-treated and tortured and disappeared mostly Sunni men from areas where ISIS was active and failed to respect their due process and fair trial rights".[24] The report also states that there has been "torture during interrogations by Iraqi forces as a method to extract confessions instead of carrying out robust criminal investigations".[25] Amnesty International notes that Iraqi courts "continued to admit 'confessions' that were extracted under torture as evidence. Many of those convicted after these unfair and hasty trials were sentenced to death".[26] Where allegations of torture were made, "most judges did not take any action to investigate the allegations".[27]

18. NSIRA notes that the 2017 MD definition of substantial risk specifies that the threshold of "substantial risk" may be met at a lower level of probability where the risk is of severe harm. This is especially relevant in countries, such as Iraq, where serious and systemic human rights abuses take place.

19. The 2011 and 2017 MDs set out that a substantial risk of mistreatment is one that is "personal, present and foreseeable". In assessing the "foreseeability" element, DND/CAF has stated that:

---

[22] This will trigger reporting requirements pursuant to Section 4 of Annex A of the Ministerial Direction to the Department of National Defence and the Canadian Armed Forces: Avoiding Complicity in Mistreatment by Foreign Entities, November 24, 2017.
[23] DND/CAF review comments provided to NSIRA via e-mail on February 5, 2020.
[24] Human Rights Watch: World Report 2019: Events of 2018, pp. 297-301.
[25] *Ibid.*
[26] Amnesty International Report 2017/18: The State of the World's Human Rights, pp. 202-205.
[27] *Supra* 13.

"…for a risk to be considered foreseeable, the risk must be such that a reasonable person, with the reasonably available information at the time of sharing, would foresee mistreatment as a consequence of said sharing. Foreseeability is assessed based on all facts available at the time of sharing, and must constantly be reassessed as situations change or new information is received. In addition, to be "substantial", the risk must be real and based on something more than theory or speculation. To be foreseeable, the mistreatment must occur as a causal consequence of the sharing of information."[28] *(emphasis added)*

20. The importance of the "causal consequence" is illustrated by DND/CAF's concept of the "air gap", which it has used when sharing information in Iraq. The "air gap" was described as follows:

> "CAF provides information to PF [Partner Forces] that is used in identifying a point of interest. This information could result in the issuance of arrest warrants. Individuals taken into custody would be subject to a detention hearing before a judge, within 72 hours.
>
> That is the point after which the Iraqi judicial process takes over using evidence obtained solely by Iraqi assets. Canadian information could not be used in the indictment of individuals.
> ."[31]

21. DND/CAF has explained that it relies on caveats requiring that their information not be used beyond the warrant point in the proceeding.[32] As a result of the "air gap", "any further actions taken by Iraqi Officials in respect of a detainee, independent of the CAF disclosed information, remains theoretical and speculative, which in accordance with the MD, does not meet the threshold of substantial risk, as it includes foreseeability".[33] DND/CAF thus does not appear to consider itself obligated to factor the longer-term risk of subsequent mistreatment into its determinations of "substantial risk" when assessing proposed instances of information sharing, despite the systemic risk of severe mistreatment in Iraqi detention, as any such mistreatment would not be a "causal consequence" of DND/CAF information sharing and thus not foreseeable.

---

[28] *Supra* 13.

[29] "The Canadian Special Operations Forces (CANSOFCOM) is a high-readiness organization, able to deploy special operations forces on very short notice to protect Canadians from threats at home and abroad. CANSOFCOM provide the Chief of the Defence Staff (CDS) with agile, highly special operations forces." www.canada.ca/en/special-operations-forces-command.html

[31] Record of Discussion, – Information Sharing, 5 November 2018. The Commander of CANSOFCOM does note that the "threshold for detaining someone is high" and that "a very small percentage of those arrested in the operation are actually detained".

[32] DND/CAF briefing to NSIRA on February 10, 2020.

[33] *Supra* 13.

22. DND/CAF emphasized to NSIRA that, in practice, it monitors

, and assesses the human rights situation on an ongoing basis. DND/CAF indicated that it would not ignore specific information regarding the mistreatment

Such precautions are important and noteworthy. But they do not replace the full case-by-case assessment of substantial risk required by the 2017 MD. **NSIRA observes that while DND/CAF's interpretation of foreseeability is multi-faceted, the requirement for there to be a "causal consequence between the information sharing with an entity and the potential mistreatment that could occur" runs the risk of narrowing the definition of substantial risk, and therefore the application of the 2017 MD.**[36]

23. A definitive examination of DND/CAF's information sharing under Operation IMPACT was outside the scope of this review, and NSIRA has reached no conclusions regarding DND/CAF's information sharing in the context of Operation IMPACT. Given its importance, however, NSIRA may return to this issue in a future review.

[34] *Supra* 32.
[35] *Ibid.*
[36] *Supra* 13.

ANNEX H: GLOBAL AFFAIRS CANADA

I BACKGROUND

1. On December 14, 2017, Global Affairs Canada (GAC) was issued Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities (the 2017 MD). GAC had not received the Ministerial Direction on Information Sharing with Foreign Entities (the 2011 MD) issued to a number of other departments.

II THE 2017 MINISTERIAL DIRECTION

Policies and Procedures

Human Rights Reports

2. GAC currently has 178 missions in 110 countries across the globe. This international footprint gives GAC unique exposure to the human rights situations around the world. GAC maintains an extensive set of Human Rights Reports that provide overviews of the human rights situation in specific countries, as well as the status of civil, political, economic and cultural rights. These reports also note the outcomes of the United Nations' Universal Periodic Reviews of human rights. All sections are supported by specific analysis and provide recommendations for engagement. The reports are not updated at fixed intervals, but rather based on operational needs. In practice, however, several are updated each year.[1] The reports are classified.[2]

3. These reports assist GAC and Canada's security and intelligence agencies in assessing the risks of sharing information with a given country.[3] Indeed, the 2011 MD explicitly noted that GAC's human rights reports could be used as a mechanism "to help ensure a consistent understanding of the risks of sharing information with foreign entities".[4] In 2018, GAC added a new mandatory sub-section to their human rights reports addressing issues of mistreatment.[5]

---

[1] GAC briefing for NSIRA, November 8, 2019.
[2] GAC has stated that due to the nature of information contained in the reports, and the potential effect that publishing the reports could have on Canada's foreign relations, the reports remain classified and unpublished. GAC Briefing for NSIRA, November 8, 2019.
[2] *Supra* 1.
[3] *Supra* 1.
[4] 2011 Ministerial Direction on Information Sharing with Foreign Entities (CBSA, CSIS, RCMP), s. 6.
[5] GAC Human Rights Reports Guidelines April 2018 – March 2019.

4. Using GAC's Human Rights Report (2019) as an example, NSIRA observes that the section on mistreatment, while brief, provides some discussion of mistreatment pertaining to individual government entities within the country. This report was drafted pursuant to GAC's new Human Rights Report Guidelines which specifically note that "details on the human rights practices of the various police and security and intelligence entities of countries, and, where possible, units within these organizations would be of tremendous benefit to the clients within the Government of Canada".[6] Previously, GAC's human rights reports had tended to describe the country as a whole.[7]

The Ministerial Direction Compliance Committee (MDCC)

5. On December 14, 2018, GAC established the Ministerial Direction Compliance Committee (MDCC).[8] The MDCC is GAC's formal "mechanism to review the potential disclosure, request or use of information in cases in which prohibitions under the MD may be engaged".[9] The MDCC is chaired by the Executive Director of the Threat Assessment and Intelligence Services Division (IDS) and includes several other senior officials from across the department, as well as a member of the GAC Legal Services unit.[10] The MDCC meets on an *ad hoc* basis when a case is brought forward. The first MDCC meeting took place on May 24, 2019.[11]

6. The MDCC is supported by a secretariat from IDS. After receiving a non-urgent request, the secretariat has five business days to gather information, including the relevant human rights reports and assessments from other Government of Canada departments such as CSE, CSIS, and the RCMP, in order to prepare for the meeting.[12]

7. Once convened, the MDCC discusses the human rights assessment of the country, the risk of mistreatment, and potential mitigation strategies such as caveats and assurances. **NSIRA observes that the caveat and assurance analysis guidelines included in the MDCC Terms of Reference are thorough and provide a good framework for MDCC discussions. They also reflect the state of the law expressed by the Supreme Court of Canada in *India v. Badesha*.**[13]

8. Following the meeting, a Record of Decision (RoD) is drafted and the decision passed to the requesting branch. When the MDCC is unable to determine whether the

---

[6] *Ibid.* Annex 1, pg. 7.
[7] *Supra* 5, GAC Human Rights Report 2019.
[8] GAC response to NSIRA questions, e-mail dated November 26, 2019.
[9] Terms of Reference – Committee on Compliance with Ministerial Direction to Global Affairs Canada: Avoiding Complicity in Mistreatment by Foreign Entities ("Ministerial Direction Compliance Committee").
[10] Members include the Directors General of the Human Rights Freedoms and Inclusion (IOD) branch; Consular Operations (CND); Security and Emergency Management (CSD); Geographic Coordination and Mission Support (NMD); Legal Affairs (JLD); the relevant Geographic Bureau; as well the Senior Counsel of the National Security Law Team. Terms of Reference – Committee on Compliance with Ministerial Direction to Global Affairs Canada: Avoiding Complicity in Mistreatment by Foreign Entities ("Ministerial Direction Compliance Committee").
[11] *Supra* 9.
[12] *Supra* 1, 9.
[13] *India v. Badesha*, 2017 SCC 44, [2017] 2 SCR 127.

substantial risk of mistreatment can be mitigated and the sponsor still wishes to share the information, the matter is referred to an Assistant Deputy Minister-level committee for consideration. If this committee is unable to make a determination, the matter is referred to the Deputy Minister.[14]

9. Sections 23 and 25 of the 2017 MD require GAC to report annually to the Minister on the implementation of the MD and to file a public copy of the report. **NSIRA observes that GAC fulfilled the requirement to report to the Minister. An unclassified version of the report has not yet been publically released.**[15]

Process

10. The MDCC Terms of Reference explain that when a Director General (DG) or a Head of Mission (HoM) wishes to share information that "presents the potential for substantial risk of mistreatment" they must bring the case to MDCC.[16] This presupposes that the DG has assessed the information sharing with regard to the risk of mistreatment that it creates. In early 2018, a message was broadcast to all GAC employees announcing the issuance of the 2017 MD and describing the obligations contained therein.[17] Beyond this message, however, GAC lacks a written policy or process requiring that employees assess all potential instances of information sharing entailing a risk of mistreatment and that notable cases be brought to the attention of senior management. GAC employees also lack guidance regarding how the risk of mistreatment and the threshold of substantial risk are to be assessed. **Given these gaps, NSIRA observes that GAC has not yet fully implemented the 2017 MD. In particular, GAC has not fulfilled its obligations under s. 19 of the 2017 MD** "to maintain policies and procedures for assessing risks associated with relationships with foreign entities".

11. The MDCC Terms of Reference include an exigent circumstances provision intended for use in cases involving an imminent threat to a GAC mission or in response to a critical incident abroad. In exigent circumstances, decisions regarding information sharing are exempted from consideration by the MDCC. GAC personnel must nonetheless assess the risk of mistreatment posed by the information sharing as required by MD. Specifically, personnel must "consult JUS [the GAC Legal Services unit] for specific advice, when possible, on how to handle information in their possession

---

[14] Ministerial Direction Compliance Committee: Outline of Process and Roles.

[15] GAC has stated that the report was provided to the Minister on April 5, 2019, and no public copy has been published yet as the report is pending approval by the Minister of Foreign Affairs. Additionally, no copy has been shared with NSICOP as per the2017 MD. *Supra* 8.

[16] Ministerial Direction Compliance Committee: Outline of Process and Roles.

[17] Annual Report 2017-2018, Ministerial Direction to Global Affairs Canada: Avoiding Complicity in Mistreatment by Foreign Entities. In June 2018, a follow-up message was sent to the members of the Global Security Reporting Program (GSRP) explaining the need for their reporting to comply with the obligations of the 2017 MD. There is no indication that this was followed by any specific guidelines regarding how to implement the requirements of the 2017 MD in the context of that program. See e-mail from o GSRP, Monday, June 18, 2018. When asked, GAC suggested that GSRP officers do not share information but rather collect it. GSRP officers were, however, among the first GAC employees given training on the 2017 MD. GAC briefing for NSIRA, November 8, 2019.

and seek approval from as high a level as feasible from within their functional unit (i.e., Head of Mission). General JUS guidelines may also be relied upon when obtaining case-specific legal advice is not possible due to imminent threat".[18]

12. GAC informed NSIRA that the exigent circumstances provision has never been invoked.[19] NSIRA did not analyze this process in detail, but nonetheless notes the importance of providing GAC personnel with clear direction regarding the circumstances and threshold required to invoke this provision.

III CASE STUDY

13. As of November 5, 2019, two cases had been referred to the MDCC. NSIRA reviewed documents for both cases and selected one for discussion here. The case chosen involved the sharing of information by Canadian officials in Canada's ambassador to is based in but also serves as Canada's ambassador to . In itself, the most senior person at Canada's mission in is the *Chargé d'Affaires*, who reports to the ambassador in

14. The case involved a Canadian living in been confiscated by the local police. The Canadian became irate that GAC Consular Affairs would not assist in retrieving the and proceeded to make threats against Canada's mission and the police by phone and on Facebook.[20]

15. On August 19, 2019, the ambassador in e-mailed GAC headquarters to inform them of her plan to call the Chief of Police for The ambassador also mentioned that information about the threat had been shared with in , which is co-located with Canada's mission.[21]

16. Upon receipt of the e-mail, GAC officials identified the issue as one that engages the 2017 MD. GAC officials replied immediately and instructed the ambassador not to disclose the Canadian citizen's information to the police and to await further guidance from Ottawa.[22] Although the ambassador complied, she noted that she had "strong concerns that these instructions undermine [her] duty of care for staff and that [she] believes HQ is taking risks with their safety at a juncture where the threat seems very real and urgent".[23]

---

[18] *Supra* 9.
[19] *Supra* 1.
[20] E-mail from (CSD) CSS) CSW), Re: Threat to Security of Telcon with Chief of Police. August 19, 2019.
[21] *Ibid.*
[22] E-mail from to Re: Threat to Security of Telcon with Chief of Police. August 20, 2019 at 4:07 a.m.
[23] E-mail from . August 19, 2019, 7:29 p.m.

17. No attention was paid, however, to the nature and extent of the information communicated to the Upon request, NSIRA was informed that the *Chargé d'Affaires* in with a description of the threat, the passport details of the person who had made the threat, as well as a picture of the individual from Facebook.[24] This information was shared without any caveats or assurances that the information would not be further shared with the police without Canada's permission.[25] In fact did speak to the loca police "who promised to step up diplomatic security", though whether passed along enough information to identify the Canadian is not known.[26] **NSIRA observes that GAC should have either referred the case to the MDCC for a mistreatment risk assessment, or ensured that any information provided to included appropriate caveats regarding further dissemination.**

18. GAC has stated that "in the context of the moment, the first concern of the Chargé d'Affaires was her duty of care to the mission"

19. Meanwhile, GAC officials in Ottawa moved quickly to consult the RCMP, CSIS and CSE. The RCMP pointed out that mission security was not an RCMP issue, but provided its country report.[28] CSIS, for its part, could not provide any information as they did not have an information sharing agreement with [29] while CSE did not provide its country report as it was not up-to-date.[30] On August 19, GAC convened an MDCC meeting to discuss the case. The MDCC agreed that sharing the information with entailed a substantial risk of mistreatment, but they also identified several mitigation measures, including:

i. "Outreach by HOM to the Chief of Police and local police seeking documented assurances that the CANCIT will be accorded due process and that, if detained, he would not be mistreated and Canada would receive unimpeded consular access to him";

---

[24] *Supra* 8. This determination directly contravenes

Supra 8.

[26] *Supra* 8.

[28] E-mail from to and RE: Draft Record of Decision: Committee on Compliance with Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities, August 20, 2019. Also e-mail from to , RE: MDCC on avoiding complicity on Mistreatment, August 20, 2019.

[29] E-mail from to RE: Contact details for consult. August 19, 2019.

[30] *Supra* 8.

ii. "RCMP follow-up with contacts in the law enforcement community to reinforce the HoM's messages"; and

iii. "Ongoing Mission follow-up with the local police".[31]

20. The MDCC RoD stated that "the Secretariat completed outstanding requests for information from partner agencies. There was no substantial risk of mistreatment identified by the RCMP, CSE or CSIS".[32] **NSIRA observes that this statement does not accurately reflect the responses from these agencies, as none provided an assessment of the risks specific to the case.**

21. On August 21, 2019, the RoD was sent to the HoM in to which a response was received on August 22, 2019, stating that the HoM was in the process of seeking assurances.[33] MDCC did not follow-up on this case until October 22, 2019, at which point the HoM explained that "in the end, we did not disclose the Cancit's name to the police or any authority" as appropriate assurances were not received and the situation "had calmed down".[34]

22. GAC has noted that while the MDCC is not obliged to follow-up on the outcome of their recommendations, they intend to integrate such a requirement into the next iteration of the MDCC ToR as such follow-up "would be a useful lessons learned tool for MDCC members".[35] **NSIRA observes that follow-up is crucial to ensuring ultimate accountability for decisions made and any information shared.**

---

[31] E-mail from to RE: Record of Decision: Committee on Compliance with Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities (MDCC). August 21, 2019.
[32] NSIRA flagged these issues during a briefing on November 5, 2019. GAC later amended the RoD to address the errors regarding CSIS and CSE, but not the RCMP. E-mail from GAC to NSIRA RE: Follow up questions (Review of the implementation of Avoiding Complicity in Mistreatment by Foreign Entities Act), December 24, 2019.
[33] E-mail from to RE: Record of Decision: Committee on Compliance with Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities (MDCC). August 21, 2019.
[34] E-mail from to RE: Record of Decision: Committee on Compliance with Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities (MDCC). October 22, 2019.
[35] *Supra* 8.

ANNEX I: THE CANADA BORDER SERVICES AGENCY

I BACKGROUND

1. The Canada Border Services Agency (CBSA) administers over ninety acts, regulations and international agreements at Canada's borders. The two primary statutes that govern CBSA's activities are, however, the *Immigration and Refugee Protection Act* (IRPA) and the *Customs Act*. In addition, much of the information sharing conducted by the CBSA is governed by specific Memoranda of Understanding (MoUs) with foreign entities as well as other Government of Canada departments. Of the CBSA's foreign information sharing, the majority occurs with Canada's Five Eyes partners.[1]

2. On September 9, 2011, CBSA was issued the Ministerial Direction on Information Sharing with Foreign Entities (the 2011 MD). In October 2011, an interim MD implementation policy was issued. In 2012, this was followed by the "Policy on Implementing the Ministerial Direction to the CBSA on Information Sharing with Foreign Entities".

3. NSIRA was informed that much of the information CBSA shares with foreign entities is routine and low risk.[2] The CBSA's operations are very broad, however, and entail varied and voluminous information sharing with foreign entities. Given the human rights records of many countries, it is unlikely that *none* of CBSA's information sharing will involve a risk of mistreatment. For instance, the CBSA:

- discloses information "to facilitate removals by engaging local authorities in foreign countries and embassies/consulates in Canada";[3] and

- supports "inland enforcement investigations by working with foreign country authorities to obtain information essential to building a case for an inadmissibility hearing or enforcement case".[4]

4. With regard to the deportation process, CBSA has explained that it relies largely on quasi-judicial or judicial bodies to determine if there is a substantial risk of mistreatment. For instance, CBSA might execute removal orders that rely on the Immigration Review Board (IRB) to make determinations regarding the associated risks.[5] While the risk of mistreatment related to the removal itself falls within the purview

---

[1] Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities: Briefing for the National Security and Intelligence Review Agency Secretariat, November 1, 2019.
[2] *Ibid*.
[3] *Ibid.*
[4] *Ibid.*
[5] *Ibid.*

of the IRB, the CBSA's information sharing with foreign entities may take place in situations where individuals do not have recourse to the IRB. For instance, individuals overseas may not have recourse to the IRB. These cases could trigger CBSA's obligations pursuant to the 2017 MD.

5. NSIRA was informed that CBSA has not conducted a formal survey of its information sharing with foreign entities to identify those areas or classes of information sharing that could result in a risk of mistreatment occurring.[6]

II THE 2017 MINISTERIAL DIRECTION

6. On September 25, 2017, CBSA received the Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities (the 2017 MD).

7. Sections 24 and 26 of the MD require CBSA to report annually to the Minister on the implementation of the MD and to file a public copy of the report. **NSIRA observes that these requirements were fulfilled. The Minister was provided a classified report and the public report was published on the CBSA website.**[7]

Policies and Procedures

8. In response to the 2017 MD, CBSA issued new guidance. "The Policy and Operational Guidelines for the Ministerial Direction to the CBSA: Avoiding Complicity in Mistreatment by Foreign Entities" came into effect on September 1, 2018, eleven months after CBSA received the 2017 MD.

9. The document discusses in general terms the recording and reporting requirements contained in the MD. The document states that "CBSA officials implicated in a disclosure (or request for information) decision may manage these risks with due diligence using appropriate risk assessment and analysis procedures as set out in their own processes".[8] No such processes were provided to NSIRA.

10. Notably, CBSA drafted a document entitled "Performing Assessments of the Risk of Mistreatment by Foreign Entities for your Information Sharing Activity"[9] that discusses how CBSA would sort countries into tiers based on the level of mistreatment risk posed,

---

[6] CBSA briefing to NSIRA, January 22, 2019.
[7] https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/md-dm/md-dm-17-18-eng.html
[8] The Policy and Operational Guidelines for the Ministerial Direction to the CBSA: Avoiding Complicity in Mistreatment by Foreign Entities. 2018.
[9] Performing Assessments of the Risk of Mistreatment by Foreign Entities for your Information Sharing Activity. November 2018.

and then triage information sharing accordingly. NSIRA was informed that these guidelines have not been finalized or implemented.[10]

11. **NSIRA observes that CBSA has not provided guidance to assist CBSA officers in identifying information sharing that could result in a substantial risk of mistreatment or guidance regarding how to mitigate such risks. In addition, CBSA has not fulfilled the requirement in s. 20 of the 2017 MD to "maintain internal policies and procedures for assessing the risks associated with the relationships with foreign entities".**

12. The absence of risk assessment guidelines results in two issues of concern:

1) Decisions regarding risk and mitigation become contingent on the individual officer's personal judgement. Even the best-informed and best-intentioned officer will not be aware of the full range of risks and contextual considerations needed to rigorously assess the risk of mistreatment posed by any instance of information sharing.

2) Decisions are made by officers who may have a direct operational interest in the sharing of information, which may therefore result in a lack of independence and objectivity.

13. The CBSA policy suite focusses mainly on information sharing pursuant to s. 107 of the *Customs Act* and s. 8 of the *Privacy Act*.[11] CBSA's analysis of the sharing of information under the *Privacy Act* does not discharge or bypass its responsibilities regarding the risk of mistreatment under the MD.[12] Along similar lines, the existence of an MoU with a foreign entity does not eliminate the need to assess the mistreatment risks of sharing information.

14. In October 2018, CBSA established an inbox to provide officers with guidance should they require assistance regarding issues related to information sharing. CBSA employees are actively using this resource.[13]

---

[10] CBSA informed NSIRA that these supporting guidelines were never implemented. CBSA also indicated that they rely heavily on the country reports from the RCMP and Global Affairs Canada, but CBSA policies do not refer to these reports or to their use. CBSA briefing to NSIRA, November 1, 2019.
[11] Policy on the Disclosure of Customs Information: Section 107 of the Customs Act, December 20, 2012. Policy on the Disclosure of Personal Information: Section 8 of the Privacy Act. December 17, 2013.
[12] CBSA has stated that the majority of its disclosures occur pursuant to the *Customs Act* and the *Privacy Act.* CBSA briefing to NSIRA on November 1, 2019.
[13] CBSA Disposition Table, in response to draft review, received by NSIRA on February 7, 2020.

Process

15. Annex A to CBSA's 2018 policy and operational guidelines sets out the process to be followed in situations where a CBSA officer is "unable to determine if the situation [involving a substantial risk of mistreatment] can be mitigated":[14]

A. An officer, who has identified an instance of proposed information sharing where there is a substantial risk of mistreatment and is unsure whether the risk can be mitigated, contacts the Information Sharing and Collaborative Arrangements Policy (ISCAP) unit for guidance.

B. The CBSA business area involved in the proposed sharing of information drafts a detailed Mistreatment Risk Assessment, which includes details regarding the information to be provided or requested, the risks associated with sharing the information, possible mitigation strategies, and the outcomes of internal consultations.

C. The business area drafts a briefing note to the attention of the President and Executive Vice President of CBSA "explaining the background and considerations for information action in question".

D. The business area drafts letters to the National Security and Intelligence Committee of Parliamentarians (NSICOP) and the Minister. The letters explain the CBSA's decision and the associated rationale.

E. Once the above products are complete, the CBSA business area sends the package to CBSA's Chief Privacy Officer (CPO) and ISCAP.

F. The package is reviewed by ISCAP, the CPO, and CBSA Legal Services. Comments and feedback are provided. Both the CPO and Legal Services also prepare their own assessment of the proposed information sharing.

G. Following the above steps:

    a. If the business area no longer wishes to proceed with the sharing of information, the process ends.

    b. If the business area wishes to proceed and is supported by the CPO, the CPO will route the final package to the President of the CBSA.

    c. If the business area wishes to proceed without the support of the CPO, the business area will keep the CPO and Legal Services apprised of their progress.

[14] The Policy and Operational Guidelines for the Ministerial Direction to the CBSA: Avoiding Complicity in Mistreatment by Foreign Entities: Annex A: Operational Guidelines for Engaging the MD. September 18, 2018.

H. The final package reaches the President for decision. If the sharing of the information is approved, the President sends the previously drafted letters to the Minister and NSICOP. Regardless of the outcome, the business area sends a copy of the full information package to the CPO for record keeping.

16. **NSIRA observes that the above process is lengthy and complex.** One risk posed by a lengthy process is that the branch may be inclined to avoid referring difficult decisions to the President, and will instead make all decisions internally. Such considerations are currently theoretical, however, as CBSA has informed NSIRA that the process described above has not yet been invoked.[15] Given the volume of information that CBSA shares with foreign entities, that this process has not yet been invoked in the year since it was published likely reflects the broader gaps in policies and processes regarding information sharing noted above. Accordingly, **NSIRA observes that CBSA has not yet operationalized the 2017 MD.** CBSA informed NSIRA, however, that it is planning to introduce significant improvements over the coming year.

[15] *Supra* 1.