

National Security and Intelligence
Review Agency



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

UNCLASSIFIED

**REVIEW OF DEPARTMENTAL IMPLEMENTATION OF THE
AVOIDING COMPLICITY IN
MISTREATMENT BY FOREIGN ENTITIES ACT FOR 2019
(NSIRA REVIEW 2020-03)**

16 December 2020

TABLE OF CONTENTS

I	EXECUTIVE SUMMARY	3
II	AUTHORITIES	5
III	INTRODUCTION	5
	Review background.....	5
	Focus of the Act	5
	Review objectives	7
	Methodology and assessment focus.....	7
	Summary of the results table	8
IV	FINDINGS AND RECOMMENDATIONS	9
	Realities of Implementation for 2019.....	9
	Importance of establishing operational frameworks.....	9
	Community coordination and best practices	10
	Framework application inconsistency	12
	Country and entity assessments	13
V	CONCLUSION	14
	ANNEX A: Summary of departmental responses and NSIRA assessments	16
	1. Requirements under the Act	16
	2. Requirements under the Orders in Council.....	17
	2.1 Disclosure of information.....	17
	2.2 Request for information	18
	2.3 Use of information	19
	3. Application and record keeping.....	20
	4. Country and entity assessments	21
	ANNEX B: Findings and Recommendations	22
	ANNEX C: Example of the directions sent to departments.....	23
	ANNEX D: Request for information questionnaire.....	28
	ANNEX E : Recommendations from NSIRA review 2019-06	33

I EXECUTIVE SUMMARY

1. (U) The *Avoiding Complicity in Mistreatment by Foreign Entities Act* (Avoiding Complicity Act or Act) and its associated directions seek to prevent the mistreatment of any individual as a result of information exchanged between a Government of Canada department and a foreign entity. At the heart of the directions is the consideration of substantial risk, and whether that risk, if present, can be mitigated or not. To do this, the Act and the directions lay out a series of requirements that need to be met or implemented when handling information. This review covers the implementation of the directions sent to 12 departments and agencies¹ from their date of issuance, September 4, 2019, to the end of the previous calendar year, December 31, 2019. It was conducted under subsection 8(2.2) of the *National Security and Intelligence Review Agency Act* (NSIRA Act), which requires NSIRA to review, each calendar year, the implementation of all directions issued under the Act.
2. (U) While this was the inaugural annual review under the NSIRA Act, it builds upon previous work in this area undertaken by NSIRA and its predecessor SIRC.² NSIRA's review on the 2017 Ministerial Direction on information sharing with Foreign Entities is an example. The results from this previous review were sent to applicable departments³ in July 2020⁴. NSIRA is building upon this previous review and strongly supports the findings and recommendations within it.⁵ As of the date of this report, departmental responses have not been received regarding the recommendations provided in NSIRA's July 2020 Ministerial Direction review.
3. (U) It was essential to ensure that both NSIRA and the departments being reviewed met their obligations under the Avoiding Complicity Act and the *NSIRA Act*. The approach used to gather information during a global pandemic was purposely designed for this first and unique review period.
4. (U) To capture a complete view on the departmental implementation, NSIRA requested information that related directly to every department's specific obligations under the Act and the directions. The responses and associated information captured departmental activities related to the Act during the review period, and what procedures, policies, tools, etc. (*frameworks*) were leveraged to support these activities. NSIRA believes that having a robust framework is an essential part of an effective implementation of the directions departments have received.
5. (U) Beyond the specific requirements of implementation, the information provided by the departments also helped to identify gaps, considerations for best practices, and the work departments have undertaken since the review period to build and formalize their frameworks. This information and knowledge will help set up the foundation for future reviews and assist efforts on creating consistent implementation across departments. While many of the issues discussed in this report go beyond the specific requirements of the directions, their consideration is critical to the overall improvement of the implementation process and how departments ultimately support the Act. No case studies were undertaken for this review. However, the information gathered has helped establish a baseline for

1 For the 2019 review period, the 12 departments/agencies that received directions under the Avoiding Complicity Act were the Canada Border Services Agency (CBSA), Canada Revenue Agency (CRA), Canadian Security Intelligence Service (CSIS), Communications Security Establishment (CSE), Department of Fisheries and Oceans Canada (DFO), Department of National Defence and Canadian Armed Forces (DND/CAF), Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Global Affairs Canada (GAC), Immigration, Refugees, and Citizenship Canada (IRCC), Public Safety Canada (PS), the Royal Canadian Mounted Police (RCMP) and Transport Canada (TC).

2 See NSIRA review 2019-06, and SIRC reviews 2015-03 and 2017-01 as examples.

3 The departments in receipt of the 2017 Ministerial Direction were CBSA, CSE, CSIS, DND/CAF, GAC and RCMP.

4 This date was previously indicated as February 2020. It now reflects the date of the official ministerial correspondence for this review.

5 See Annex E for the full recommendations from this review.

overarching issues the community is facing. Building on this, future reviews will begin to examine specific sharing framework challenges and questions and look closely at specific cases and departmental legal opinions to guide review findings.

6. (U) While NSIRA was pleased with the considerable efforts made by many departments new to the Avoiding Complicity Act in building up their supporting frameworks, it was clear during this review that departments are employing very different approaches to guide their information handling activities. The responses received demonstrate various inconsistencies across the departments. Having a consistent and coordinated approach when addressing the concerns related the Act is not a requirement for implementation, however, NSIRA believes that there is value in such an approach. And while departments will always require unique aspects in their sharing frameworks to address the unique characteristics of their mandates and activities, to improve the implementation process, a goal all involved likely have, the identification and sharing of best practices is critical.

7. (U) For example, determining the best means for having a unified approach when engaging with foreign entities of concern or ensuring that an information sharing activity is consistently evaluated for risk by all departments. The recommendations provided on these issues in this review capture what NSIRA believes to be important concerns and considerations for supporting and improving departmental implementation.

8. (U) Additionally, as the directives received under the Act do not describe the specific means by which departments 'implement' them, it is incumbent on the community to ensure that they have sufficiently robust frameworks and programs in place to fully support an assertion of implementation. Therefore, the information gathered during this review went beyond a strict assessment of implementation, but also considered the aspects required to better support this implementation. Going forward, this approach will help establish the foundation for subsequent reviews. Drawing on the findings and concerns identified here, NSIRA will continue to consider aspects that will ultimately improve underlying frameworks, thereby supporting an improved implementation of the Act across the community.

II AUTHORITIES

9. (U) This review was conducted under subsection 8(2.2) of the NSIRA Act, which requires NSIRA to review, each calendar year, the implementation of all directions issued under the Avoiding Complicity Act.

III INTRODUCTION

Review background

10. (U) In 2011, the Government of Canada implemented a general framework for *Addressing Risks of Mistreatment in Sharing Information with Foreign Entities*. The framework aimed to establish a coherent and consistent approach across government when sharing and receiving information with Foreign Entities. Following this, Ministerial Direction was issued to applicable departments in 2011 on *Information Sharing with Foreign Entities*, and then again in 2017 on *Avoiding Complicity in Mistreatment by Foreign Entities*.

11. (U) On July 13, 2019, the Avoiding Complicity Act came into force. This Act codifies and enshrines Canada's commitments in respect to the *Canadian Charter of Rights and Freedoms*, and Canada's international legal obligations on prohibiting torture and other cruel and inhumane treatment.

12. (U) On September 4, 2019, pursuant to section 3 of the Act, the Governor in Council (GiC) issued written directions to the Deputy Heads⁶ of the following 12 departments and agencies: Canada Border Services Agency (CBSA), Canada Revenue Agency (CRA), Canadian Security Intelligence Service (CSIS), Communications Security Establishment (CSE), Department of Fisheries and Oceans Canada (DFO), Department of National Defence and Canadian Armed Forces (DND/CAF), Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Global Affairs Canada (GAC), Immigration, Refugees, and Citizenship Canada (IRCC), Public Safety Canada (PS), the Royal Canadian Mounted Police (RCMP) and Transport Canada (TC).⁷

13. (U) The GiC issued directions focused on three aspects of handling information when interacting with a foreign entity: the disclosure of information, the requesting of information, and the use of any information received.

14. (U) Pursuant to section 7 of the Act, every Deputy Head having received direction must, before March 1 of each year, submit to the appropriate Minister a report regarding the implementation of those directions during the previous calendar year. Following this, every Deputy Head must, as soon as feasible after submitting the report, make a version of it available to the public.

Focus of the Act

15. (U) In the same spirit as the Ministerial Direction (MD) that preceded it, the Avoiding Complicity Act and its associated directions seek to prevent the mistreatment of any individual due to the

⁶ Deputy Head is as defined in Section 2 of the Act and interchanged in this report with "Deputy Minister".

⁷ While 6 of the 12 departments were specifically identified in the Act to receive the directions, the process for determining which other departments should receive directions under the Act is unclear. Beyond the scope of this review year, future reviews may consider the evaluation process for departmental inclusion for receiving directions under the Act.

exchange of information between a Government of Canada department⁸ and a foreign entity. The Act also aims to limit the use of information received from a foreign entity that may have been obtained through the mistreatment of an individual. While the previous MD guided the activities of a selection of Canada's security and intelligence departments, the Act broadened this scope to capture all departments whose interactions with foreign entities included information exchanges where such a concern may apply.

16. (U) The focus of the Act is to ensure departments take the necessary steps during their information sharing activities to avoid contributing in any way to the mistreatment of an individual. To do this, the Act and the directions lay out a series of requirements that need to be met or implemented when handling information. There is an expectation that each department will satisfy these requirements by leveraging departmentally established mechanisms and procedures, or *frameworks* that will allow each department to confidently demonstrate how it has responded to its responsibilities under the Act.

17. (U) During the first year that the Act was in force, written directions using nearly identical language were sent to the Deputy Heads of 12 departments.⁹ In regard to disclosure, the directions read as follows:

"If the disclosure of information to a foreign entity would result in a substantial risk of mistreatment of an individual, the Deputy Head must ensure that Department officials do not disclose the information unless the officials determine that the risk can be mitigated, such as through the use of caveats or assurances, and appropriate measures are taken to mitigate the risk."

18. (U) With respect to requesting information, the directions state:

"If the making of a request to a foreign entity for information would result in a substantial risk of mistreatment of an individual, the Deputy Head must ensure that Department officials do not make the request for information unless the officials determine that the risk can be mitigated, such as through the use of caveats or assurances, and appropriate measures are taken to mitigate the risk."

19. (U) Lastly, as it relates to the use of information, the directions indicate:

"The Deputy Head must ensure that information that is likely to have been obtained through the mistreatment of an individual by a foreign entity is not used by the Department

(a) in any way that creates a substantial risk of further mistreatment;
(b) as evidence in any judicial, administrative or other proceeding; or
(c) in any way that deprives someone of their rights or freedoms, unless the Deputy Head or, in exceptional circumstances, a senior official designated by the Deputy Head determines that the use of the information is necessary to prevent loss of life or significant personal injury and authorizes the use accordingly."

20. (U) At the heart of the directions is the consideration of substantial risk¹⁰, and whether that risk, if present, can be mitigated or not. This determination is done on a case-by-case basis.¹¹ Each

⁸ Department is as defined in Section 2 of the Avoiding Complicity Act.

⁹ Please see Annex C for a complete example of the directions sent to departments.

¹⁰ While the Act does not define substantial risk, a number of departments continue use the definition contained in the 2017 Ministerial Direction. The lack of the Act's definition of 'substantial risk' was an issue raised in NSIRA's review 2019-06.

¹¹ Further defining what constitutes a "case" will be helpful in determining how it should be evaluated. For example, sharing single pieces of information vs. bulk data, or sharing personal vs non-personal information.

department is responsible for making these determinations as it applies to its activities. Following the outcome of a department's determination of these important questions, cases may be approved, denied, or elevated to the Deputy Head for consideration. For the latter cases, this then results in additional reporting requirements for the Deputy Head. Throughout this process, there is also a requirement to ensure the accuracy, reliability, and limitations of use of all information being handled.

Review objectives

21. (U) After the Avoiding Complicity Act came into force in July 2019, the Governor in Council's written directions were sent to each applicable department in September 2019. The period for this year's review is September 4, 2019 to December 31, 2019. The short timeframe (approximately 4 months) associated with this year's review means that departments are being assessed, in large part, on what they would *already* have had in place to address risks of mistreatment associated with information sharing, or what they were able to implement in a four-month window. NSIRA is cognizant that for the departments that were not previously subject to the 2017 MD¹² on *Avoiding Complicity in Mistreatment by Foreign Entities*, the timeframe to implement the written directions was somewhat limited, as it would have been challenging to create and operationalize new procedures such that they would be reflected in the department's activities during the period being reviewed.

22. (U) While it was essential to ensure that both NSIRA and the departments being reviewed met their obligations, these challenges were kept in mind when evaluating the objectives for this first review. Given these considerations, the objectives of this year's review¹³ were to determine whether:

- departments had fully implemented the directions received under the Act in conformity with the obligations set out therein;
- departments had established and operationalized frameworks that sufficiently enabled them to meet the obligations set out in the Act and directions; and,
- there was consistency in implementation across applicable departments.

Methodology and assessment focus

23. (U) To capture a complete view of the departmental implementation of the Act, NSIRA constructed a series of questions related directly to every department's obligations under the Act and the directions. The responses and associated information captured what specific activities took place during the review period and what departmental frameworks were leveraged to adequately support these activities.¹⁴

24. (U) The information provided by the departments also helped to identify gaps, considerations for best practices, and the work departments have undertaken to build and formalize their frameworks to meet their obligations under the Act and directions. The information provided and the knowledge gained will help set up the foundation for future reviews and help create consistent implementation across departments.

25. (U) The method used to gather information during a global pandemic was designed for this first and unique review period. We believe it allowed departments to quickly and efficiently indicate both

12 CRA, DFO, IRCC, FINTRAC, PS, and TC were not subject to this MD.

13 These were captured in the Terms of Reference NSIRA sent to departments.

14 Please see Annex D for the request for information (RFI) questions sent to departments.

whether the directions had been implemented, and what frameworks, processes, and policies had been leveraged or put in place.

26. (U) Responses to many of the RFI questions were simply yes/no answers. Often, answers were dependent on what information handling activities took place with foreign entities by the department during the review period. As such, a number of questions could be returned with 'not applicable', and this was an acceptable response. Many of the questions were related to specific and easily defined requirements under the Act and its associated directions, e.g. 'was a report submitted to the Minister?' or 'Did the Deputy Minister inform the applicable bodies of all their decision made under the act?'

27. (U) Other questions were designed to capture the details of the underlying processes that supported a department's implementation, i.e. a department may indicate that they ensured no substantial risk of mistreatment was present in any of their information sharing activities, but how did they support this claim? Likewise, for an assertion that a possible substantial risk of mistreatment had been mitigated, what was in place that allowed a department to make this assertion? Therefore, this series of questions required sufficiently detailed responses to fully capture what a department had in place that allowed it to confidently state that it has met its implementation obligations under the Act and the issued directions.

28. (U) Finally, a portion of the questions was intended to capture the level of uniformity in implementation across departments. This includes such things as country/entity assessments, triage practices, and record keeping. Much of this information will also help with recommendations going forward. This multi-faceted approach resulted in three main areas being evaluated to assess implementation for this review period and help set the groundwork for future reviews.

- Departments have clear and comprehensive frameworks, policies, and guidelines such that they can demonstrate how they have fully implemented the directions under the Act.
- All reporting requirements associated with both the Act and its applicable directions have been met.
- Differences or gaps associate with areas such as country/entities assessments, record keeping, case triage, etc., such that consistent implementation across departments would be challenging.

Summary of the results table

29. (U) The table in Annex A captures a summary of both the departmental responses to the implementation questions and NSIRA's assessment regarding these responses. The assessment was based on the associated details provided by departments in the context of the specific information requested. As explained above, many of the responses were returned as not applicable (n/a). Since many implementation requirements are connected to specific activities, the absence of such activities would mean that the requirement does not come into play. The best example of this for the current review is the absence of any Deputy Minister level determinations. All 12 departments indicated that they did not have any cases referred to the Deputy Minister level for determination.¹⁵ All additional reporting requirements associated with this level of decision were not applicable and thus considered satisfied.

¹⁵ CSIS had two cases sent to the Director but they were subsequently withdrawn before a determination was made.

30. (U) If a specific requirement was not met, it was flagged. The relatively few instances of this were connected with departments not meeting certain reporting obligations under the Act. In all cases, the department involved pre-identified these missing requirements and indicated that efforts were underway to address them.

31. (U) The concerns and findings captured in the table (and others) are discussed subsequently. A concern was flagged in two situations: where there was an uncertainty associated with a department's ability to support their implementation requirements; and cross-cutting issues related to general aspects of all of the frameworks described, both of which led to the findings and recommendations proposed.

IV FINDINGS AND RECOMMENDATIONS

Realities of Implementation for 2019

32. (U) A challenge for departments for this first review was associated with one of the assessment items listed above, i.e. whether they had established frameworks to demonstrate how they supported the implementation of the directions they received.

33. (U) With the Avoiding Complicity Act coming into force in July 2019, it was not feasible that departments would create and stand-up new frameworks for information exchanges in time for the period being reviewed. Although the Act did specify several Deputy Heads that were to receive directions, it only included those who received the previous 2017 MD. The remaining new departments received their directions in September 2019. Regardless of this two-month difference, each department would have been required to rely on, to some extent, existing procedures when handling information sharing with foreign entities during the review period.

34. (U) This put the departments that had previously formalized policies and processes at an advantage when implementing the directions. For those departments who were not subject to the previous 2017 MD on information sharing, NSIRA considered how they leveraged and adjusted what was already in place to respond to their new responsibilities under the Act. What we then expected to see, for all departments, was what subsequent steps were taken during the review period and afterwards, to either adjust or create frameworks to better meet implementation requirements going forward. NSIRA noted that in response to questions¹⁶ on frameworks for handling information and mitigating risk, several of the departments new to the considerations of the Act provided extensive detail on their efforts and progress on building out their frameworks to support the directives.¹⁷ References to having these frameworks formalized over the subsequent year were also encouraging.

35. (U) **Finding no. 1: NSIRA found that several departments, new to the considerations of the Act, described considerable progress being made during the review period and afterwards to build out formalized frameworks to support implementation.**

Importance of establishing operational frameworks

36. (U) As discussed, having fully established operational frameworks in place for this review period may not have been feasible for the departments that did not previously have processes to support their activities. This, however, did not exempt a department from the requirements of implementation. Each department was still expected to leverage what it currently had in place to properly address the

¹⁶ See Annex D for questions requesting framework descriptions.

¹⁷ The efforts as described by CRA, DFO, FINTRAC, and IRCC to build out their departmental frameworks in their associated responses.

concerns associated with the Avoiding Complicity Act. Furthermore, there was a logical follow-on expectation that departments would take subsequent steps to build out formal frameworks to address any perceived gaps to support the implementation of the Act going forward if necessary.

37. (U) After reviewing the responses received, NSIRA is concerned that departments with minimal information sharing activities taking place during their operations have yet to address the necessity of having a robust framework in place, regardless of how often that framework is leveraged.¹⁸ For example, although PS and TC may primarily act as facilitators or coordinators for information exchanges on specific programs¹⁹, they are still interacting with foreign entities,²⁰ and therefore are required to fully assess their interactions with a foreign entity in this regard.

38. (U) If a department without a formal framework assesses that it has few or no cases associated with the Act, then it may believe it is adequately positioned to address any sharing concerns should they arise. This, however, is not the case. Even single instances of information exchange in which the concerns of the Act may apply require a framework to support it properly. In many cases, it will be the framework itself that properly identifies whether a sharing activity raises concerns under the Act. If there is no formal process in place, then this identification becomes problematic. Simply saying that there are no cases or activities associated with the Act is not sufficient. That determination can only be made after a sharing activity is scrutinized through the lens of a robust framework. Going forward, all departments who receive directions should demonstrate a formal framework that ensures all information sharing activities are adequately evaluated against the considerations of the Act.

39. (U) **Finding no. 2: NSIRA found that departments conducting minimal information exchanges with foreign entities have not yet fully addressed the importance of having an official information sharing framework in place.**

Recommendation no. 1: NSIRA recommends that all departments in receipt of directions under the Act have an official framework that ensures they can fully support their implementation of the directions.

Community coordination and best practices

40. (U) While departmental coordination and the sharing of best practices are not a requirement of the Avoiding Complicity Act or the directions, NSIRA considered such an approach's value. What became clear during this first review was that every department employs a very different framework to guide their information sharing activities with foreign entities. This is to be expected to some extent, given the different mandates, sharing requirements, and areas of focus associated with each department. However, these differences are also a reflection of the independent, internal development that has taken place for the different frameworks being used. While the departments receiving

18 The summary table in Annex A captures concerns associated with frameworks in this regard, specifically on the current frameworks described by PS and TC. PS has indicated that efforts are underway to formalize its processes and policies associated with the Act, however the lack of detail provided on this effort was the cause of concern.

19 The passenger protect program (PPP) is coordinated by PS, and actioned by TC with input from other departments.

20 While concerns were flagged on what TC has in place with respect to its framework to support the directions, this was primarily due to the lack of detail provided in procedural policy provide. As with all departments, further framework evaluation will provide a better assessment of its ability to support the implementation of the directions.

directions under the Act do interact on this subject to some extent,²¹ to date, based on the responses provided, it appears that the majority of the work done by the departments to build supporting frameworks to address their responsibilities associated with the Act have been done so independently.²² There was little to no overlap with how departments described the various aspects of their frameworks, even amongst the departments subject to the earlier MD on this issue.

41. (U) There would be value in departments collectively identifying the key aspects common or required in all information exchanges with foreign entities and then working together to craft best practices, irrespective of what a department currently has in place. This process should draw on all available resources to make this determination. Each department can then turn to their existing frameworks to consider where and how they can be adjusted to match this community-agreed upon ideal. This is not to say that aspects of what a department already has in place in their framework will not ultimately be seen as the best practice. Several departments do have robust sharing frameworks in place, and these will contribute significantly to this exercise. However, arriving at this determination independently will provide an additional level of confidence.

42. (U) Department-specific challenges, of course, cannot be ignored. In fact, they will weigh in strongly on such a conversation. Departments share information under their mandates for various reasons, and this will mean that coordination on certain aspects of a sharing framework may not be possible. However, this needs to be evaluated. It is important that what already exists, or what is hard change, does not unduly influence what may be best. This approach will create uniformity (where possible) across the community and provide a starting point for 'must haves' for each department to evaluate their existing processes against.

43. (U) The Public Safety Information Sharing Coordination Group (ISCG) was established to support departments on information sharing. As such, it is in an ideal position to help mitigate issues arising from the lack of coordination. Leading such efforts would build on the work already being done by this group. During recent discussions with NSIRA, the ISCG indicated that the tracking of lessons learned and the sharing of best practices was not yet routine. Going forward, there would be value in a more coordinated effort when departments are updating/changing their framework. Ensuring that this coordination takes place will require support and leadership by senior-level officials. This will help in sharing best practices once identified, and establish more consistent approaches across departments.

44. (U) **Finding no. 3: NSIRA found that the differences and variability in departmental frameworks demonstrate a previous lack of coordination across the community and a need to identify best practices.**

Recommendation no. 2: NSIRA recommends that departments coordinate to identify best practices for all essential components of information sharing frameworks and that the ISCG is leveraged to ensure these practices are shared where possible across the community to support the implementation of the Act.

²¹ The ISCG is the only official mechanism of coordination on this issue that we're aware of. As it was established fairly recently, its role in coordinating development on existing departmental frameworks would have been minimal.

²² A number of departments do leverage country and entity assessments developed by other departments, however overall, the framework descriptions as provided by departments capture a vast variety of approaches, tool, and processes being used.

Framework application inconsistency

45. (U) A series of questions in this review was related to aspects of consistency in how departments apply their frameworks.²³ From this series, a comparison was made on how many times an information sharing/use event triggered an evaluation of any kind against the considerations of the Avoiding Complicity Act, versus how many of these triaged cases were elevated or referred up for decision. The results helped gauge two important aspects of a framework: One, the threshold requirements, i.e. how often a sharing activity triggers an evaluation of any kind; and two, the decision making power given to the operators who are initially handling these activities.

46. (U) The feedback and the responses received demonstrate potential inconsistencies in both aspects across departments. For example, several departments indicated zero cases as being triaged/evaluated under the concerns of the Act during the review period²⁴, yet also specified that they are involved in regular information sharing or, specified that no information received from foreign entities was derived from mistreatment. These responses appear to be inconsistent as it would be problematic to participate in information sharing or to make such mistreatment determinations without the activity being evaluated on some level.

47. (U) Other departments indicated a larger number of cases as initial triaged/evaluated, but also indicated that none of them were elevated in their decision making process for higher-level decisions.²⁵ This would seem to suggest that all determinations were being made at the operational level. Such a result puts significant weight on the operator and the initial assessment tools they are leveraging if they are making all determinations independently. This reinforces the importance of a robust framework to help make these determinations, as previously indicated in Finding no. 2. As a result of these differences, potential challenges arise on accurately assessing the volume of cases being handled by departments, the tracking of those cases deemed to present a substantial risk, those which can be mitigated for, and those where the risk was not found to be substantial or even present.

48. (U) These responses may result from how each department defines a 'case' or how it records a case, or they may be a result of differences in how a department's decision-making process is leveraged. NSIRA's concern is that these differences may indicate an inconsistency in application thresholds at different departments. As such, the following results were viewed as a potential issue based on the responses received:

- if a department was involved in any kind for information exchange with a foreign entity during the review period, but did not indicate that any cases were formally triaged/evaluated; or
- if there was a significant number of cases triaged, but none were elevated to a higher level for determination.

49. (U) Such results do not necessarily indicate a problem as aspects of a framework may be able to account for this, however, looking further into how and why the department's framework produced these outcomes is important. Future reviews will be able to do this. Consistent initial steps for information sharing activities, including triage/evaluation thresholds and documentation, are critical to the effective application of a framework, and ultimately to identifying best practices.

²³ See section 3 questions on *Application and Record Keeping* in the summary table in Annex A.

²⁴ DFO, IRCC, PS, and TC all indicated that they had no cases evaluated/triaged. See question 3.1 in the summary table in Annex A.

²⁵ This included CBSA and CRA, both who have Frameworks in place that include processes to escalate the decision making process.

50. (U) **Finding no. 4: NSIRA found that there are inconsistencies in the application of existing sharing frameworks between departments, specifically concerning information evaluation thresholds, and decisions being elevated for senior level determinations.**

Recommendation no. 3: NSIRA recommends that departments establish consistent thresholds for triggers in their information sharing frameworks, including initial evaluations against the concerns of the Act, when a case is to be elevated in the decision process, and how this is documented.

Country and entity assessments

51. (U) A key recommendation of NSIRA's previous review on information sharing²⁶ related to the country/entity assessments being used by departments to inform their decision making process when sharing or using information with a foreign entity. While the use of country/entity assessments is not a required aspect of implementing the directions under the Act, NSIRA continues to support this tool as an important aspect of any sharing framework. In its previous review, NSIRA determined that having a firm grasp on the human rights situation, as well as any other pertinent information associated with a country/entity, was essential to making an informed decision on whether there should be concerns, caveats, or limitations when handling information with that country/entity. Moreover, having such information captured to ensure all departments consistently approach these countries/entities is critical. At the time of the previous review, the following recommendation was made:

Departments should develop:

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

52. (U) It is important to note that there has been no formal response from departments on this previous recommendation as of the date of this report. Furthermore, during this report, two departments continue to raise concerns with NSIRA's stance on this issue during the consultation process.²⁷ While NSIRA continues to support this recommendation, as explained below, further discussions with departments on how to approach this matter may be warranted, specifically on the distinction between how this recommendation may apply to a foreign country/entity vs a specific foreign partner a department may be dealing with.

53. (U) Based on the responses provided on this topic for the current review period²⁸, there is still inconsistency in this area. While almost all departments indicated that country/entity assessments were a standard part of their framework²⁹, the responses also indicate differences in which country

²⁶ NSIRA review 2019-06.

²⁷ During the consultation process CSE and PS indicated they had concerns related to NSIRA's recommendations on country and entities assessments.

²⁸ Section 4, *Country and Entity Assessments* in the summary table in Annex A captures the assessment of the departments in this area.

²⁹ Public Safety and Transport Canada do not yet have a process for this.

assessments are used, how they are leveraged, and who is responsible for updating them.³⁰ For example, several departments rely on their own in-house created assessments, while others leverage the assessments created by Global Affairs Canada and others. While departments who indicated that they are leveraging country/entity assessment tools in their process also indicated that these assessments captured human rights concerns, this has yet to be independently evaluated. NSIRA is concerned that these differences could result in different approaches/stances being taken by departments when dealing with the same foreign entity. While the country/entity assessments tools themselves are *not necessarily* in question³¹, the fact that every department is not leveraging or does not have access to all useful or applicable information is.

54. (U) NSIRA remains of the view that having a consistent stance on all countries and entities when implementing the requirements of the Act is important. Issues such as mistreatment and human rights should not be decided at a departmental level, but on a whole-of-government level. While mindful of classification levels, ensuring all departments have access to the same relevant information associated with a foreign country/entity is critical to making an informed decision. Due to the nature of their work, departments may be privy to unique information on a country/entity, some or all of which can be shared. This would lead to fully informed assessments that allow for a consistent approach when dealing with any country/entity. In addition to improving duplication of effort in this area by departments, NSIRA continues to see standardized country and entity assessments, which can be accessed and contributed to by all departments, as key to moving toward a more consistent and effective implementation of the Act across the community.

55. (U) **Finding no. 5: NSIRA found a lack of unification and standardization in the country and entity assessments being leveraged by departments, resulting in inconsistencies in approach/stance by the community when interacting with Foreign Entities of concern related to the Act.**

Recommendation no. 4: NSIRA recommends that departments identify a means to establish unified and standardized country and entity risk assessment tools to support a consistent approach by departments when interacting with Foreign Entities of concern under the Act.

V CONCLUSION

56. (U) While aspects of implementation can be easily quantified and evaluated e.g. reporting requirements to a Minister, others, which support implementation are more difficult to measure, e.g.:

- What does a sufficiently robust framework for assessing and mitigating risk when sharing with a foreign entity look like?
- Does this depend on the specific requirements and activities of the department; or,
- Are there steps that should always be involved when vetting a foreign entity under the considerations of the Act?

³⁰ The main assessment tools being leveraged by the departments were created and managed by RCMP and GAC, however, multiple secondary sources, both government and independent, are often used as well.

³¹ The in-house managed country/entity assessments of RCMP and FINTRAC appear to be robust.

57. (U) Measuring and weighing the answers to such questions is challenging. They are more nuanced, and can't be as easily quantified. Regardless, they must be considered and addressed. Drawing on the considerations and concerns identified in this review will help departments to ask the questions that will improve their underlying frameworks with the following goals in mind:

- To identify the essential/key elements that need to be a part of any framework for it to address the concerns associated with the Avoiding Complicity Act sufficiently; and,
- To have all identified best practices implemented as consistently as possible across departments.

58. (U) Future reviews will push towards these goals by seeking answers to those questions above. By looking more closely at specific case studies, departmental legal opinions, items of inconsistency, and the departmental frameworks that are already demonstrating best practices that should be shared. Ultimately the results of such efforts will contribute to improving the implementation of the Act across the community.

ANNEX A: Summary of departmental responses and NSIRA assessments

	Satisfied
	Concerns
	Missing requirement
na	Not applicable

*The information captured in this summary and assessment table is current to the date of this report.

*This table previously captured references to the information and responses from departments used to make our assessments. While the assessments remain, these references have been removed from the table resulting in 'empty' or nil squares.

		CBSA	CRA	CSE	CSIS	DFO	DND	FINTRAC	GAC	IRCC	PS	RCMP	TC
1. Requirements under the Act													
1.1	Did the Deputy Minister make the directions received under the Orders in Council available to the public?	yes	no	yes	yes	yes	yes						
1.2	Was a copy of the directions received under the Order in Council provided to NSICoP, NSIRA, and if applicable, the Civilian Review and Complaints Commission for the RCMP?	yes	no	yes	yes	yes	yes	yes	no	yes	yes	yes	yes
1.3	Was a report on the implementation of directions received under the Order in Council submitted to the appropriate Minister? If so, when was it submitted?	yes Mar 2020	yes Feb 2020	yes Feb 2020	yes Feb 2020	yes Feb 2020	yes Sep 2020	yes Feb 2020	yes Jul 2020	yes Mar 2020	yes Mar 2020	yes Feb 2020	yes Feb 2020
1.4	Was the report that was submitted to the Minister made available to the public?	no	yes	yes	yes	yes	no	yes	no	yes	yes	yes	yes
1.5	a) Did the Minister provide a copy of the report they received to NSICoP, NSIRA, and if applicable, the Civilian Review and Complaints Commission for the RCMP?	yes	yes	yes	yes	yes	no	yes	no	yes	yes	yes	yes
	b) Was all information that the above parties were not entitled to see removed from the copies provided?	yes	yes	yes	yes	yes	na	na	na	na	yes	yes	yes

		CBSA	CRA	CSE	CSIS	DFO	DND	FINTRAC	GAC	IRCC	PS	RCMP	TC
2. Requirements under the Orders in Council													
2.1 Disclosure of information													
2.11	a) Is there a framework for deciding whether the disclosure of information to a foreign entity would result in a substantial risk of mistreatment of an individual?	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	yes	yes
	b) Please describe the framework used to make this decision. In doing so please include all steps from when the information to be disclosed is identified, to where a decision is made on whether there is a risk associated with disclosing the information. This should include, but is not limited to the personnel, tools (country/entity assessments), committees, etc. involved in the process.												
2.12	a) Is there a framework for determining whether an identified substantial risk of mistreatment due to a disclosure of information can be mitigated?	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	yes	no
	b) Please describe the framework used to make this determination. In doing so please include all steps from when a substantial risk of mistreatment due to disclosure is identified, to where a determination is made on whether that risk can be mitigated or not. This should include, but is not limited to the personnel, tools (caveats, assurances, or appropriate measures), committees, etc. involved in the process.												
2.13	Were all cases where there was an inability by officials to determine whether the risk of mistreatment could be mitigated referred to the Deputy Minister?	na	na	na	yes	na	na	na	na	na	na	na	na
2.14	a) For cases where the Deputy Minister determined that the risk of mistreatment due to disclosure could be mitigated, what measures were taken to mitigate the risk?	na	na	na	na	na	na	na	na	na	na	na	na
	b) Was the basis of this determination clearly outlined and documented?	na	na	na	na	na	na	na	na	na	na	na	na

		CBSA	CRA	CSE	CSIS	DFO	DND	FINTRAC	GAC	IRCC	PS	RCMP	TC
2.15	a) Were all disclosures of information where the risk of mistreatment could be mitigated accompanied by a characterization of the information's accuracy and reliability? ³²	na	na	na	na	na	na	na	na	na	na	na	na
	b) What is the process used to determine this accuracy and reliability?				na	na		na	na		na		na
2.16	Was the Minister, NSIRA, and NSICoP informed of all determinations by the Deputy Minister to disclose information, and was all additional information considered in making the determination also provided?	na	na	na		na	na	na	na	na	na	na	na
2.2 Request for information													
2.21	a) Is there a framework for deciding whether a request for information from a foreign entity would result in a substantial risk of mistreatment of an individual	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	yes	yes
	b) Please describe the framework used to make this decision. In doing so please include all steps from when the information to be requested is identified, to where a decision is made on whether there is a risk associated with requesting the information. This should include, but is not limited to the personnel, tools (country/entity assessments), committees, etc. involved in the process.												
2.22	a) Is there a framework for determining whether an identified substantial risk of mistreatment due to a request for information can be mitigated?	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	yes	na
	b) Please describe the framework used to make this determination. In doing so please include all steps from when a substantial risk of mistreatment due to a request for information is identified, to where a determination is made on												na

³² In the case of CSE, the information must be accurately and reliably reflective of the intelligence product from which it was obtained.

		CBSA	CRA	CSE	CSIS	DFO	DND	FINTRAC	GAC	IRCC	PS	RCMP	TC
	whether that risk can be mitigated or not. This should include, but is not limited to the personnel, tools (caveats, assurances, or appropriate measures), committees, etc. involved in the process.												
2.23	Were all cases where there was an inability by officials to determine whether the risk of mistreatment could be mitigated referred to the Deputy Minister?	na	na	na	na	na	na	na	na	na	na	na	na
2.24	a) For cases where the Deputy Minister determined that the risk of mistreatment due to a request for information could be mitigated, what measures were taken to mitigate the risk?	na	na	na	na	na	na	na	an	na	na	na	na
	b) Was the basis of this determination clearly outlined and documented?	na	na	na	na	na	na	na	na	na	na	na	na
2.25	Was the Minister, NSIRA, and NSICoP informed of all determinations by the Deputy Minister to request information, and was all additional information considered in making the determination also provided?	na	na	na		na	na	na	na	na	na	na	na
2.3 Use of information													
2.31	a) Is there a framework for determining whether information being used by the department is likely to have been obtained through the mistreatment of an individual by a foreign entity?	yes	yes	no	yes	yes	yes	yes	no	yes	no	yes	no
	b) Please describe the framework used to make this determination. In doing so please include all steps from when the information to be used is identified, to where a decision is made on whether it was likely to have been obtained through mistreatment. This should include, but is not limited to the personnel, tools (country/entity assessments), committees, etc. involved in the process.												
2.32	For information determined likely to have been obtained through the mistreatment of an individual by a foreign entity, what controls are in place to ensure that it is	na	na	na		na		na		na	na	na	na

		CBSA	CRA	CSE	CSIS	DFO	DND	FINTRAC	GAC	IRCC	PS	RCMP	TC
	not used in following situations: (i) in any way that creates a substantial risk of further mistreatment (ii) as evidence in any judicial, administrative or other proceeding (iii) in any way that deprives someone of their rights or freedoms, unless the Deputy Minister or, in exceptional circumstances, a senior Department of Transport official designated by the Deputy Minister determines that the use of the information is necessary to prevent loss of life or significant personal injury and authorizes the use accordingly.												
2.33	a) Is information that is likely to have been obtained through the mistreatment of an individual by a foreign entity assessed for accuracy and reliability before it is used?	yes	na	yes	yes	yes	yes	yes	yes	yes	yes	yes	na
	b) How was the information's accuracy and reliability determined?		na			na	na	na		na	na	na	na
2.34	Did all authorizations for use, referred to in question 2.32, situation (c) above, accurately describe the information being used, characterize the information's accuracy and reliability, and identify the limited purpose for which the authorization was given?	na	na	na	na	na	na	na	na	na	na	na	na
2.35	Was the Minister, NSIRA, and NSICoP informed of all decisions made by Deputy Minister to authorize the use of information in a question 2.32, situation (c) above, and was all additional information considered in making the decision also provided?	na	na	na	na	na	na	na	na	na	na	na	na
3. Application and record keeping													
3.1	a) How many cases were triaged/evaluated this year?	52	60	91	not known	0	not known	60	4	0	0	15	0
	b) Did these cases reveal any gaps in the framework?	no				na	no			na	na		na
	c) If so, was the framework adjusted accordingly, and how?	na	yes	na	yes	na	na	yes	yes	na	na		na
3.2	What number of total triaged cases were	0	0	6	na	0	not	60	2	0	0	0	0

		CBSA	CRA	CSE	CSIS	DFO	DND	FINTRAC	GAC	IRCC	PS	RCMP	TC
	referred to senior management/committee?						known						
3.3	How is incoming information potentially derived from mistreatment initially marked/identified?												na
3.4	For all cases - are you retroactively able to determine when, how and why a decision was made through your record keeping system?	yes	yes	yes		yes		yes		yes	na	yes	na
4. Country and entity assessments													
4.1	Is there an established process of referral to country assessments when information is being used or exchanged with a foreign entity?	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	yes	
4.2	Did the department establish its own country assessments or work with other departments?	both	other	own	both	other	both	own	own	other	other	own	na
4.3	Are the country assessments reflective of the human rights situation in that country	See Finding #5 for comment											
4.4	Beyond country-level assessments, does the department use entity-specific caveats and assurances?	yes	no	yes	yes	yes	yes	yes	yes	yes	no	yes	na
4.5	Is the department aware of NSIRA's recommendation to unify country and entity assessments across government, as outlined in NSIRA's previous review of the 2017 Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities? ³³	yes	yes	yes	yes	no	yes	yes	yes	no	yes	yes	na

³³ This question was to gauge awareness of NSIRA's previous recommendation on this issue. NSIRA's concern on this is not department-specific but relates to the general need for attention on this issue.

ANNEX B: Findings and Recommendations

Finding no. 1: NSIRA found that several departments, new to the considerations of the Act, described considerable progress being made during the review period and afterwards to build out formalized frameworks to support implementation.

Finding no. 2: NSIRA found that departments conducting minimal information exchanges with foreign entities have not yet fully addressed the importance of having an official information sharing framework in place.

Finding no. 3: NSIRA found that the differences and variability in departmental frameworks demonstrate a previous lack of coordination across the community and a need to identify best practices.

Finding no. 4: NSIRA found that there are inconsistencies in the application of existing sharing frameworks between departments, specifically concerning information evaluation thresholds, and decisions being elevated for senior level determinations.

Finding no. 5: NSIRA found a lack of unification and standardization in the country and entity assessments being leveraged by departments, resulting in inconsistencies in approach/stance by the community when interacting with Foreign Entities of concern related to the Act.

Recommendation no. 1: NSIRA recommends that all departments in receipt of directions under the Act have an official framework that ensures they can fully support the implementation of the directions.

Recommendation no. 2: NSIRA recommends that departments coordinate to identify best practices for all essential components of information sharing frameworks and that the ISCG is leveraged to ensure these practices are shared where possible across the community to support the implementation of the Act.

Recommendation no. 3: NSIRA recommends that departments establish consistent thresholds for triggers in their information sharing frameworks, including initial evaluations against the concerns of the Act, when a case is to be elevated in the decision process, and how this is documented.

Recommendation no. 4: NSIRA recommends that departments identify a means to establish unified and standardized country and entity risk assessment tools to support a consistent approach by departments when interacting with Foreign Entities of concern under the Act.

ANNEX C: Example of the directions sent to departments

(As sent to Public Safety, however all departments received similar Orders in Council.)

PC Number: 2019-1310

Date: 2019-09-04

Her Excellency the Governor General in Council, on the recommendation of the Minister of Public Safety and Emergency Preparedness, pursuant to subsection 3(1) of the *Avoiding Complicity in Mistreatment by Foreign Entities Act*, issues the annexed *Directions for Avoiding Complicity in Mistreatment by Foreign Entities (Deputy Minister of Public Safety and Emergency Preparedness)*.

Sur recommandation du ministre de la Sécurité publique et de la Protection civile et en vertu du paragraphe 3(1) de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*, Son Excellence la Gouverneure générale en conseil donne les *Instructions visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères (sous-ministre de la Sécurité publique et de la Protection civile)*, ci-après.

Directions for Avoiding Complicity in Mistreatment by Foreign Entities (Deputy Minister of Public Safety and Emergency Preparedness)

Disclosure of information

1 (1) If the disclosure of information to a foreign entity would result in a substantial risk of mistreatment of an individual, the Deputy Minister of Public Safety and Emergency Preparedness must ensure that Department of Public Safety and Emergency Preparedness officials do not disclose the information unless the officials determine that the risk can be mitigated, such as through the use of caveats or assurances, and appropriate measures are taken to mitigate the risk.

Referral to Deputy Minister

(2) If the officials are unable to determine whether the risk can be mitigated, the Deputy Minister must ensure that the matter is referred to the Deputy Minister for determination.

Authorization by Deputy Minister

(3) If the Deputy Minister determines that the risk can be mitigated, the Deputy Minister may authorize the disclosure of the information on condition that the Deputy Minister clearly documents the basis for that determination and appropriate measures are taken to mitigate the risk.

Accuracy and reliability

(4) The Deputy Minister must ensure that information is not disclosed under subsection (1) or (3) unless it is accompanied by a characterization of the information's accuracy and reliability, as determined by the Department of Public Safety and Emergency Preparedness.

Request for information

2 (1) If the making of a request to a foreign entity for information would result in a substantial risk of mistreatment of an individual, the Deputy Minister of Public Safety and Emergency Preparedness must ensure that Department of Public Safety and Emergency Preparedness officials do not make the request for information unless the officials determine that the risk can be mitigated, such as through the use of caveats or assurances, and appropriate measures are taken to mitigate the risk.

Referral to Deputy Minister

(2) If the officials are unable to determine whether the risk can be mitigated, the Deputy Minister must ensure that the matter is referred to the Deputy Minister for determination.

Authorization by Deputy Minister

(3) If the Deputy Minister determines that the risk can be mitigated, the Deputy Minister may authorize the making of the request for information on condition that the Deputy Minister clearly documents the basis for that determination and appropriate measures are taken to mitigate the risk.

Use of information

3 (1) The Deputy Minister of Public Safety and Emergency Preparedness must ensure that information that is likely to have been obtained through the mistreatment of an individual by a foreign entity is not used by the Department of Public Safety and Emergency Preparedness

(a) in any way that creates a substantial risk of further mistreatment;

(b) as evidence in any judicial, administrative or other proceeding; or

(c) in any way that deprives someone of their rights or freedoms, unless the Deputy Minister or, in exceptional circumstances, a senior Department of Public Safety and Emergency Preparedness official designated by the Deputy Minister determines that the use of the information is necessary to prevent loss of life or significant personal injury and authorizes the use accordingly.

Precautions

(2) The Deputy Minister must ensure that the Department of Public Safety and Emergency Preparedness assesses the accuracy and reliability of the information before it is used and that any authorization given for the purposes of paragraph (1)(c) accurately describes the information, characterizes the information's accuracy and reliability and identifies the limited purpose for which the authorization is given.

Information to Minister, Agency and Committee

4 (1) The Deputy Minister of Public Safety and Emergency Preparedness must inform the Minister of Public Safety and Emergency Preparedness, the National Security and Intelligence Review Agency and the National Security and Intelligence Committee of Parliamentarians of any determination made under subsection 1(2) or 2(2) and of any decision regarding whether to give an authorization referred to in paragraph 3(1)(c), and must disclose any information considered in making the determination or decision, as soon as feasible after the determination or decision is made.

Ongoing investigation

(2) Information relating directly to an ongoing investigation carried out by a law enforcement agency may be disclosed once the investigation is no longer ongoing.

Limitation

(3) Only information to which the National Security and Intelligence Review Agency and the National Security and Intelligence Committee of Parliamentarians are entitled to have access under section 9 of the *National Security and Intelligence Review Agency Act* and section 13 of the *National Security and Intelligence Committee of Parliamentarians Act*, respectively, may be disclosed to those entities under this section.

Instructions visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères (sous-ministre de la Sécurité publique et de la Protection civile)

Communication de renseignements

1 (1) Le sous-ministre de la Sécurité publique et de la Protection civile veille, à l'égard de tout renseignement dont la communication à une entité étrangère entraînerait un risque sérieux que de mauvais traitements soient infligés à un individu, à ce que les fonctionnaires du ministère de la Sécurité publique et de la Protection civile ne communiquent le renseignement que si les fonctionnaires concluent que le risque peut être atténué, notamment par la formulation de réserves ou l'obtention de garanties, et que si les mesures d'atténuation indiquées sont prises.

Renvoi de la question au sous-ministre

(2) Si les fonctionnaires ne sont pas en mesure d'établir s'il est possible d'atténuer le risque, le sous-ministre veille à ce que la question lui soit référée pour qu'il en décide.

Autorisation du sous-ministre

(3) Le sous-ministre peut autoriser la communication du renseignement si le sous-ministre conclut que le risque peut être atténué, à condition que le sous-ministre expose clairement les motifs de sa décision et que les mesures d'atténuation indiquées soient prises.

Exactitude et fiabilité

(4) Le sous-ministre veille à ce que la communication de renseignements visée aux paragraphes (1) ou (3) ne s'effectue que si une caractérisation de leur exactitude et de leur fiabilité effectuée par le ministère de la Sécurité publique et de la Protection civile y est jointe.

Demande de renseignements

2 (1) Le sous-ministre de la Sécurité publique et de la Protection civile veille à ce que les fonctionnaires du ministère de la Sécurité publique et de la Protection civile ne fassent de demande de renseignements, à une entité étrangère, qui entraînerait un risque sérieux que de mauvais traitements soient infligés à un individu, que s'ils concluent que le risque peut être atténué, notamment par la formulation de réserves ou l'obtention de garanties, et que si les mesures d'atténuation indiquées sont prises.

Renvoi de la question au sous-ministre

(2) Si les fonctionnaires ne sont pas en mesure d'établir s'il est possible d'atténuer le risque, le sous-ministre veille à ce que la question lui soit référée pour qu'il en décide.

Autorisation du sous-ministre

(3) Le sous-ministre peut autoriser la demande de renseignements si le sous-ministre conclut que le risque peut être atténué, à condition que le sous-ministre expose clairement les motifs de sa décision et que les mesures d'atténuation indiquées soient prises.

Utilisation des renseignements

3 (1) Le sous-ministre de la Sécurité publique et de la Protection civile veille à ce que les renseignements vraisemblablement obtenus par suite de mauvais traitements

infligés à un individu par une entité étrangère ne soient utilisés par le ministère de la Sécurité publique et de la Protection civile :

- a) ni de façon à engendrer un risque sérieux de mauvais traitements additionnels;
- b) ni comme éléments de preuve dans des procédures judiciaires, administratives ou autres;
- c) ni de façon à priver une personne de ses droits ou libertés, sauf si le sous-ministre, ou dans des circonstances exceptionnelles, un haut fonctionnaire du ministère de la Sécurité publique et de la Protection civile qu'il désigne, juge cette utilisation nécessaire pour éviter des pertes de vie ou des lésions corporelles et l'autorise à cette fin.

Précautions

(2) Le sous-ministre veille à ce que le ministère de la Sécurité publique et de la Protection civile évalue l'exactitude et la fiabilité des renseignements avant leur utilisation et à ce que toute autorisation donnée au titre de l'alinéa (1)c) décrive les renseignements en cause avec précision, en caractérise l'exactitude et la fiabilité et indique les limites de l'objet qu'elle vise.

Information — ministre, Office et Comité

4 (1) Le sous-ministre de la Sécurité publique et de la Protection civile informe le ministre de la Sécurité publique et de la Protection civile, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement et le Comité des parlementaires sur la sécurité nationale et le renseignement des décisions prises au titre des paragraphes 1(2) ou 2(2) et de celles qui sont relatives à l'autorisation visée à l'alinéa 3(1)c), et leur communique tout renseignement ayant servi à la prise des décisions, dès que possible après leur prise.

Enquête en cours

(2) Les renseignements liés directement à une enquête en cours menée par un organisme d'application de la loi peuvent être communiqués une fois l'enquête n'est plus en cours.

Restriction

(3) Seuls les renseignements auxquels l'Office de surveillance des activités en matière de sécurité nationale et de renseignement et le Comité des parlementaires sur la sécurité nationale et le renseignement ont le droit d'avoir accès, respectivement au titre des articles 9 de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* et 13 de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*, peuvent leur être communiqués aux termes du présent article.

ANNEX D: Request for information questionnaire**1. Requirements under the Act**

1.1	Did the Deputy Minister make the directions received under the Orders in Council available to the public? Answer:	
1.2	Was a copy of the directions received under the Order in Council provided to NSICoP, NSIRA, and if applicable, the Civilian Review and Complaints Commission for the RCMP? Answer:	
1.3	Was a report on the implementation of directions received under the Order in Council submitted to the appropriate Minister? If so, when was it submitted? Answer:	
1.4	Was the report that was submitted to the Minister made available to the public? Was the following information appropriately removed: (a) That which would be injurious to national security, national defense or international relations or compromise an ongoing operation or investigation? (b) That which is subject to solicitor-client privilege or the professional secrecy of advocates and notaries or to litigation privilege? Answer:	
1.5	a) Did the Minister provide a copy of the report they received to NSICoP, NSIRA, and if applicable, the Civilian Review and Complaints Commission for the RCMP? Answer:	
	b) Was all information that the above parties were not entitled to see removed from the copies provided? Answer:	

2. Requirements under the Orders in Council**2.1 Disclosure of information**

2.11	Is there a framework for deciding whether the disclosure of information to a foreign entity would result in a substantial risk of mistreatment of an individual? Answer:	
------	---	--

	<p>Please describe the framework used to make this decision. In doing so please include all steps from when the information to be disclosed is identified, to where a decision is made on whether there is a risk associated with disclosing the information. This should include, but is not limited to the personnel, tools (country/entity assessments), committees, etc. involved in the process.</p> <p>Answer:</p>	
2.12	<p>Is there a framework for determining whether an identified substantial risk of mistreatment due to a disclosure of information can be mitigated?</p> <p>Answer:</p> <p>Please describe the framework used to make this determination. In doing so please include all steps from when a substantial risk of mistreatment due to disclosure is identified, to where a determination is made on whether that risk can be mitigated or not. This should include, but is not limited to the personnel, tools (caveats, assurances, or appropriate measures), committees, etc. involved in the process.</p> <p>Answer:</p>	
2.13	<p>Were all cases where there was an inability by officials to determine whether the risk of mistreatment could be mitigated referred to the Deputy Minister?</p> <p>Answer:</p>	
2.14	<p>For cases where the Deputy Minister determined that the risk of mistreatment due to disclosure could be mitigated, what measures were taken to mitigate the risk?</p> <p>Answer:</p> <p>Was the basis of this determination clearly outlined and documented?</p> <p>Answer:</p>	
2.15	<p>Were all disclosures of information where the risk of mistreatment could be mitigated accompanied by a characterization of the information's accuracy and reliability?</p> <p>Answer:</p> <p>What is the process used to determine this accuracy and reliability?</p> <p>Answer:</p>	
2.16	<p>Was the Minister, NSIRA, and NSICoP informed of all determinations by the Deputy Minister to disclose information, and was all additional information considered in making the determination also provided?</p> <p>Answer:</p>	

2.2 Requests for information

2.21	<p>Is there a framework for deciding whether a request for information from a foreign entity would result in a substantial risk of mistreatment of an individual?</p> <p>Answer:</p>	
------	--	--

	<p>Please describe the framework used to make this decision. In doing so please include all steps from when the information to be requested is identified, to where a decision is made on whether there is a risk associated with requesting the information. This should include, but is not limited to the personnel, tools (country/entity assessments), committees, etc. involved in the process.</p> <p>Answer:</p>	
2.22	<p>Is there a framework for determining whether an identified substantial risk of mistreatment due to a request for information can be mitigated?</p> <p>Answer:</p> <p>Please describe the framework used to make this determination. In doing so please include all steps from when a substantial risk of mistreatment due to a request for information is identified, to where a determination is made on whether that risk can be mitigated or not. This should include, but is not limited to the personnel, tools (caveats, assurances, or appropriate measures), committees, etc. involved in the process.</p> <p>Answer:</p>	
2.23	<p>Were all cases where there was an inability by officials to determine whether the risk of mistreatment could be mitigated referred to the Deputy Minister?</p> <p>Answer:</p>	
2.24	<p>For cases where the Deputy Minister determined that the risk of mistreatment due to a request for information could be mitigated, what measures were taken to mitigate the risk?</p> <p>Answer:</p> <p>Was the basis of this determination clearly outlined and documented?</p> <p>Answer:</p>	
2.25	<p>Was the Minister, NSIRA, and NSICoP informed of all determinations by the Deputy Minister to request information, and was all additional information considered in making the determination also provided?</p> <p>Answer:</p>	

2.3 Use of information

2.31	<p>Is there a framework for determining whether information being used by the department is likely to have been obtained through the mistreatment of an individual by a foreign entity?</p> <p>Answer:</p> <p>Please describe the framework used to make this determination. In doing so please include all steps from when the information to be used is identified, to where a decision is made on whether it was likely to have been obtained through mistreatment. This should include, but is not limited to the personnel, tools (country/entity assessments), committees, etc. involved in the process.</p>	
------	--	--

	Answer:	
2.32	<p>For information determined likely to have been obtained through the mistreatment of an individual by a foreign entity, what controls are in place to ensure that it is not used in following situations:</p> <ul style="list-style-type: none"> a) in any way that creates a substantial risk of further mistreatment b) as evidence in any judicial, administrative or other proceeding c) in any way that deprives someone of their rights or freedoms, unless the Deputy Minister or, in exceptional circumstances, a senior Department of Transport official designated by the Deputy Minister determines that the use of the information is necessary to prevent loss of life or significant personal injury and authorizes the use accordingly. <p>Answer:</p>	
2.33	<p>Is information that is likely to have been obtained through the mistreatment of an individual by a foreign entity assessed for accuracy and reliability before it is used?</p> <p>Answer:</p> <p>How was the information's accuracy and reliability determined?</p> <p>Answer:</p>	
2.34	<p>Did all authorizations for use, referred to in question 2.32, situation (c) above, accurately describe the information being used, characterize the information's accuracy and reliability, and identify the limited purpose for which the authorization was given?</p> <p>Answer:</p>	
2.35	<p>Was the Minister, NSIRA, and NSICoP informed of all decisions made by Deputy Minister to authorize the use of information in a question 2.32, situation (c) above, and was all additional information considered in making the decision also provided?</p> <p>Answer:</p>	

3. Application and record keeping

3.1	<p>How many cases were triaged/evaluated this year?</p> <p>Answer:</p> <p>Did these cases reveal any gaps in the framework?</p> <p>Answer:</p> <p>If so, was the framework adjusted accordingly, and how?</p> <p>Answer:</p>	
-----	--	--

3.2	What percentage of total triaged cases were referred to senior management/committee? Answer:	
3.3	How is incoming information potentially derived from mistreatment initially marked/identified? Answer:	
3.4	For all cases - are you retroactively able to determine when, how and why a decision was made through your record keeping system? Answer:	

4. Country and entity assessments

4.1	Is there an established process of referral to country assessments when information is being used or exchanged with a foreign entity? Answer:	
4.2	Did the department establish its own country assessments or work with other departments? Answer:	
4.3	Are the country assessments reflective of the human rights situation in that country? Answer:	
4.4	Beyond country-level assessments, does the department use entity-specific caveats and assurances? Answer:	
4.5	Is the department aware of NSIRA's recommendation to unify country and entity assessments across government, as outlined in NSIRA's previous review of the 2017 Ministerial Direction on <i>Avoiding Complicity in Mistreatment by Foreign Entities</i> ? Answer:	

ANNEX E : Recommendations from NSIRA review 2019-06:

Review of Departmental Frameworks for Avoiding Complicity in Mistreatment by Foreign Entities.

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 operation personnel directly invested in the outcome.

Recommendation no. 3: Departments should develop:

- a) a unified set of assessments of the human rights situation 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.

Recommendations no. 4: The definition of “substantial risk” should be codified in law or public direction.