

File: 2200-A-2024-01



Office of
the Intelligence
Commissioner

Bureau du
commissaire
au renseignement

P.O. Box/C.P. 1474, Station/Succursale B
Ottawa, Ontario K1P 5P6
613-992-3044 • Fax 613-992-4096

INTELLIGENCE COMMISSIONER
DECISION AND REASONS

IN RELATION TO THE DETERMINATION OF CLASSES OF
ACTS OR OMISSIONS THAT WOULD OTHERWISE CONSTITUTE OFFENCES
PURSUANT TO SUBSECTION 20.1(3) OF THE
CANADIAN SECURITY INTELLIGENCE SERVICE ACT AND
SECTION 19 OF THE *INTELLIGENCE COMMISSIONER ACT*

MARCH 11, 2024

TABLE OF CONTENTS

I.	OVERVIEW	1
II.	CONTEXT	2
III.	STANDARD OF REVIEW	6
IV.	ANALYSIS	7
	i) The classes.....	8
V.	REMARKS	13
	i) The responsibility of designated CSIS employees.....	13
	<i>a. Legal considerations in relation to the responsibility of designated CSIS employees ..</i>	<i>14</i>
	<i>b. Measures in place to guide designated employees ..</i>	<i>16</i>
	<i>c. The potential for the Minister to consider other factors in his conclusions ..</i>	<i>17</i>
	ii) Impact of recent judicial decision.....	18
	iii) Additional information for the Minister	18
VI.	CONCLUSIONS	19

I. OVERVIEW

1. This is a decision reviewing the conclusions of the Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs (Minister) in relation to his determination of eight classes of acts or omissions that would otherwise be contrary to the law.
2. The *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 (*CSIS Act*) allows Canadian Security Intelligence Service (CSIS) employees designated by the Minister or other individuals acting under their direction to lawfully commit acts or omissions that would otherwise constitute offences. Set out in section 20.1 of the *CSIS Act*, this is referred to as the Justification Framework.
3. To benefit from the Justification Framework, the acts or omissions must fall within an approved class, which means a class determined by the Minister that is approved by the Intelligence Commissioner. Pursuant to the *Intelligence Commissioner Act*, SC 2019, c 13, s 50 (*IC Act*), the Intelligence Commissioner must approve the class if he is satisfied that the Minister's conclusions, on the basis of which the class is determined, are reasonable.
4. On March 15, 2023, I approved seven of the eight classes of acts or omissions that would otherwise constitute offences that had been determined by the Minister (File 2200-A-2023-02). I did not approve one of the classes on the grounds that the Minister's conclusions were not reasonable with respect to certain acts or omissions that would fall within that class. In response to the specific concerns raised in my decision, CSIS prepared a new application that was submitted to the Minister, who authorized the amended class. Following my review, I approved the amended class on June 21, 2023.
5. The *CSIS Act* requires the Minister to authorize classes at least once a year and an approved class is valid for a period of one year following the Intelligence Commissioner's approval. While the amended class is not set to expire until June 20, 2024, CSIS requested that the Minister authorize the amended class at the same time as the other seven classes approved in March 2023 for all classes to be valid for the same period.

6. On February 12, 2024, pursuant to subsection 20.1(3) of the *CSIS Act*, the Minister determined, by order, eight classes of acts or omissions that would otherwise constitute offences (Authorization).
7. On February 13, 2024, the Office of the Intelligence Commissioner received the Authorization for my review and approval under the *IC Act*.
8. Based on my review and for the reasons below, I am satisfied that the Minister's conclusions made under subsection 20.1(3) of the *CSIS Act* in relation to the eight classes of acts or omissions are reasonable.
9. Consequently, pursuant to paragraph 20(1)(a) of the *IC Act*, I approve the Minister's Authorization of the eight classes dated February 12, 2024.

II. CONTEXT

10. A detailed legislative context of the Justification Framework is set out in past decisions. In summary, the Justification Framework was added to the *CSIS Act* in 2019. It provides legal protection to the person committing the otherwise unlawful act, namely CSIS employees designated by the Minister or persons being directed by them. The Justification Framework recognizes that these individuals may be required to commit limited unlawful activity to carry out effective investigations in order to gain trust, maintain credibility and develop access to threat-related information, notably in contexts where individuals are working covertly. The addition of the Justification Framework to the *CSIS Act* was deemed necessary to modernize the legislation.
11. However, the Justification Framework does not mean that CSIS employees can disregard the rule of law. No act or omission that would infringe a right guaranteed by the *Canadian Charter of Rights and Freedoms* (*Charter*) can be committed (s 20.1(22), *CSIS Act*). Further, subsection 20.1(18) of the *CSIS Act* sets out the following six specific categories of acts or omissions designated CSIS employees, or persons directed by them, could never be justified in committing:

- a) causing, intentionally or by criminal negligence, death or bodily harm to an individual;
- b) willfully attempting in any manner to obstruct, pervert or defeat the course of justice;
- c) violating the sexual integrity of an individual;
- d) subjecting an individual to torture or cruel, inhuman or degrading treatment or punishment, within the meaning of the Convention Against Torture;
- e) detaining an individual; or
- f) causing the loss of, or any serious damage to, any property if doing so would endanger the safety of an individual.

12. While the objective of the Justification Framework is to ensure that CSIS carries out warrantless intelligence collection activities in accordance with the rule of law, it is useful to situate the Justification Framework within CSIS' intelligence collection activities to better understand how that objective is achieved.
13. CSIS may carry out warrantless intelligence collection activities pursuant to sections 12 (relating to a threat to the security of Canada) and 16 (foreign intelligence) of the *CSIS Act*. To do so, the activities must either not interfere with a reasonable expectation of privacy, or be only minimally intrusive if a reasonable expectation of privacy is engaged (for example, use of specialized equipment which reveals the country where the user's cellphone account is located). Normally, activities that are intrusive – meaning they interfere with an individual's reasonable expectation of privacy – would be unreasonable and contrary to the protection in section 8 of the *Charter* against unreasonable searches and seizures by the state. However, if intrusive activities are authorized by a reasonable law and executed reasonably, they can be lawfully conducted. Courts have found that sections 12 and 16 of the *CSIS Act*, determined to be a reasonable law, effectively render lawful such activities, as long as they are only minimally intrusive and executed reasonably (*X(Re)*, 2017 FC 1047; *Canadian Security Intelligence Service Act (RE)*, 2020 FC 697; *Canadian Security Intelligence Service Act (CA) (Re)*, 2022 FC 1444).
14. When the activities under sections 12 and 16 are more than minimally intrusive on the privacy interests of Canadians, for example conducting electronic surveillance, CSIS must

obtain a warrant from the Federal Court pursuant to section 21 of the *CSIS Act*. A warrant effectively renders lawful the collection activities CSIS conducts that interfere with a reasonable expectation of privacy, which without a warrant would be contrary to section 8 of the *Charter*. A warrant can also render lawful the supporting activities that CSIS may have to conduct to be able to carry out the collection activities.

15. Activities pursuant to the Justification Framework have the same purpose as the supporting activities, but in the context of warrantless collection activities. They facilitate intelligence collection activities carried out under sections 12 and 16 by authorizing the commission of supporting acts or omissions that would otherwise be unlawful. In that sense, they are not, strictly speaking, collection activities. They may be necessary for CSIS to collect intelligence, but the statutory authority to collect the intelligence without a warrant remains with sections 12 and 16. For example, [...] could constitute a financing terrorism offence pursuant to the *Criminal Code*. The payment, which could hypothetically fall within the Justification Framework, facilitates the acquisition of information [...], which is the collection activity.
16. Given that acts under the Justification Framework are not intelligence collection activities – and therefore do not constitute a search or seizure – they should not interfere with a reasonable expectation of privacy. Further, given that the Justification Framework explicitly prohibits the commission or direction of acts or omissions that would breach *Charter* rights, CSIS may not conduct activities that interfere with a reasonable expectation of privacy, even if the activities are minimally intrusive. Indeed, the Justification Framework does not render an otherwise intrusive activity legal.
17. Similarly, information that is collected in an operation where acts or omissions were committed or directed to be committed under the Justification Framework cannot automatically be retained by CSIS. The information must meet the statutory requirements under sections 12 or 16 to be retained.
18. It is therefore crucial for CSIS employees to understand when an activity may interfere with a reasonable expectation of privacy, as well as the distinction between activities that are only

minimally intrusive and those that require a warrant. These are so-called “red lines” that can only be crossed with the proper authorization.

19. Once a class is approved by the Intelligence Commissioner and a designated CSIS employee is satisfied the activity falls within an approved class, to commit or direct a person to commit an otherwise unlawful act, the employee must believe on reasonable grounds that the commission of the act or omission, as compared to the threat, is reasonable and proportional in the circumstances, having regard to such matters as:

- a) for section 12 activity: the nature of the threat, the nature of the act or omission and the reasonable availability of other means for performing the information and intelligence collection activity;
- b) for section 16 activity: the nature of the act or omission, the nature of the objective to be achieved and the reasonable availability of other means to achieve the objective (s 20.1(11) and (15), *CSIS Act*).

20. In accordance with section 23 of the *IC Act*, the Minister confirmed in his cover letter that he provided me with all information that was before him when determining the classes of acts or omissions. The record is therefore composed of:

- a) Briefing Note from the Director of CSIS to the Minister dated December 29, 2023, which includes 17 annexes that can be grouped into the following categories (Director’s Briefing Note):
 - i) CSIS overview defining and describing the eight classes (Overview);
 - ii) Statistical breakdown of the use of acts and omissions per class;
 - iii) *Intelligence Commissioner – Decision and Reasons*, March 15, 2023 (File 2200-A-2023-02), and June 21, 2023 (File 2200-A-2023-07);
 - iv) Ministerial Directions for Operations and for Accountability;
 - v) CSIS Operational Policies and training materials; and

- vi) Deck presentation to the Intelligence Commissioner and staff, including minutes of meeting. (I had not previously seen the minutes, but confirm that I have no concerns with their content).
- b) Briefing Note from the Deputy Minister of Public Safety to the Minister dated February 8, 2024; and
- c) Minister's Authorization of the eight classes dated February 12, 2024.

III. STANDARD OF REVIEW

21. The *IC Act* requires the Intelligence Commissioner to review whether the Minister's conclusions are reasonable. The Intelligence Commissioner's jurisprudence establishes that the reasonableness standard, as applied to judicial reviews of administrative action, applies to my review.

22. As indicated by the Supreme Court of Canada, when conducting a reasonableness review, a reviewing court is to start its analysis by examining the reasons of the administrative decision maker (*Mason v Canada (Citizenship and Immigration)*, 2023 SCC 21, para 79). In *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65, at paragraph 99, the Court succinctly describes what constitutes a reasonable decision:

A reviewing court must develop an understanding of the decision maker's reasoning process in order to determine whether the decision as a whole is reasonable. To make this determination, the reviewing court asks whether the decision bears the hallmarks of reasonableness – justification, transparency and intelligibility – and whether it is justified in relation to the relevant factual and legal constraints that bear on the decision.

23. Relevant factual and legal constraints can include the governing statutory scheme, the impact of the decision and principles of statutory interpretation. Indeed, to understand what is reasonable, it is necessary to take into consideration the context in which the decision under review was made as well as the context in which it is being reviewed. It is therefore necessary to understand the role of the Intelligence Commissioner, which is an integral part of the statutory scheme set out in the *IC* and *CSIS Acts*.

24. A review of the *IC Act* and the *CSIS Act*, as well as legislative debates, show that Parliament created the role of the Intelligence Commissioner as an independent mechanism to ensure that government action taken for the purpose of national security and intelligence was properly balanced with the respect of the rule of law and the rights and freedoms of Canadians. To maintain that balance, I consider that Parliament created my role as a gatekeeper. While reviewing the Minister's conclusions, I am to carefully examine whether the important privacy and other interests of Canadians and persons in Canada were appropriately considered and weighed as well as to ensure that the rule of law is fully respected.
25. When the Intelligence Commissioner is satisfied (*convaincu*) that the Minister's conclusions at issue are reasonable, he "must approve" the authorization (s 20(1)(a), *IC Act*). Conversely, where unreasonable, the Intelligence Commissioner "must not approve" the authorization (s 20(1)(b), *IC Act*).

IV. ANALYSIS

26. To determine a class, the Minister must conclude that the commission or the directing of the acts or omissions within that class is reasonable, having regard to: (a) CSIS' information and intelligence collection duties and functions, and, (b) any threats to the security of Canada that may be the object of information and intelligence collection activities or any objectives to be achieved by such activities (s 20.1(3), *CSIS Act*).
27. Pursuant to sections 12 and 19 of the *IC Act*, in carrying out the independent oversight role of the Intelligence Commissioner, I must conduct a quasi-judicial review of the Minister's conclusions to determine whether they are reasonable. I will now proceed with my analysis of the Minister's conclusions.

i) The classes

28. In the matter before me, the Minister determined the following eight classes of acts or omissions that designated CSIS employees may be justified in committing or directing another person to commit:

Class 1 [REDACTED]

Class 2 [REDACTED]

Class 3 [REDACTED]

Class 4 [REDACTED]

Class 5 [REDACTED]

Class 6 [REDACTED]

Class 7 [REDACTED]

Class 8 [REDACTED]

29. The Minister is seeking approval of the identical eight classes that I approved last year.

Further, the ministerial conclusions are similar to those I found reasonable when I approved those eight classes.

30. Past approval by the Intelligence Commissioner does not entail that the same classes, with the same or similar ministerial conclusions, will automatically be approved again. Indeed, every ministerial authorization is distinct and is reviewed on its own record. A number of considerations could have changed between authorizations. For example, contextual information may have changed from one year to the next; there could be developments in jurisprudence that have an impact on the Intelligence Commissioner's analysis; or there could be an issue where the Minister's or the Intelligence Commissioner's understanding has evolved.

31. Further, as established by the jurisprudence of the Intelligence Commissioner, it is important for information in the authorization, as well as supporting materials, to be updated to reflect

the current operational activities undertaken by designated CSIS employees and persons directed by them. The Minister must be provided with the best available information when determining whether to authorize the classes of otherwise unlawful acts or omissions. This information includes what classes have been used by designated employees as well as information on the acts that have been committed pursuant to the Justification Framework. How acts or omissions of a class have been undertaken in the past may be a factor in determining whether a class is reasonable.

32. Similarly, from one year to the next, the Intelligence Commissioner may consider how the Minister has addressed past remarks when determining the reasonableness of his conclusions, and this should be reflected in the record.
33. In sum, the fact that the same classes have been approved in the past does not change the legal requirements that have to be satisfied for the Intelligence Commissioner to find the Minister's conclusions reasonable. Indeed, the record should reflect the fact that it is a new and distinct authorization.

ii) Updated record

34. Although the record is similar to the one provided to me in 2023, the current materials contain new information which addresses the concerns and remarks made in my 2023 decisions:
- a) In response to my remark in the March 2023 decision on the need to provide updated examples of acts committed under the Justification Framework, CSIS provided new specific examples for each class. The new examples highlight the value of the approved class in relation to a threat to the security of Canada as well as the nature of the potential information or intelligence collected.
 - b) In the March 2023 decision, I remarked that the Minister referred to a Ministerial Direction and the "policy framework" used to guide CSIS employees which were not included in the record. In this record, CSIS added operational policies related to the Justification Framework and approved classes as well as the Ministerial Directions

for Operations and for Accountability. In addition, the record includes statistical breakdown of authorizations and directions issued by class and type of threat investigation and a report broadly describing the acts or omissions committed by employees during the past fiscal year.

- c) I had raised concerns in March 2023 about how certain acts that fall within approved classes could potentially lead to a breach of the limitations set out in subsection 20.1(18) of the *CSIS Act*. For example, [...] I recommended that the Minister's conclusions be explicit about how the statutory limitations apply and fit within the decision-making process of designated CSIS employees who must determine whether a potential act or omission falls within a class and whether there are reasonable grounds to believe that the commission of the act or omission is reasonable and proportional.

In response, the Director's Briefing Note indicates that employees designated under the Justification Framework must successfully complete mandatory training and those seeking a renewed or new designation must complete an annual mandatory recertification e-training module, which is updated yearly. Employees' understanding of the application of the framework and its limitations is evaluated through practical exercises and scenarios. The training materials were enclosed in the record. In addition, CSIS included its policy on [...] explaining CSIS' operational approval and reporting processes with a view to reinforce designated employees' awareness of the statutory limitations. As per the policy, designated CSIS employees must confirm, prior to committing, or directing a person to commit, an act under the Justification Framework, that they have considered the six statutory limitations as well as the rights and freedoms guaranteed by the *Charter* and (ss 20.1(18) and (22), *CSIS Act*). As indicated in the Minister's conclusions, the policy "reinforces the designated employee awareness of the legal limitations in the regime throughout the decision making process".

- d) In my June 2023 decision, I also made a remark about CSIS' continued use of Class [...] approved by the former Intelligence Commissioner in July 2022 after I had not approved the same class in March 2023. I was of the view that relying on the "old" class could raise legal and compliance issues and that CSIS should provide the Federal Court with this context if relying on intelligence derived from activities that could fall within the "old" class. In the record before me, the Director confirmed in his Briefing Note to the Minister that when material to a warrant application before the Federal Court, CSIS has been "proactively providing the Federal Court with additional context when any information or intelligence derived from activities that fell under the previous Class [...]".

iii) The Minister's conclusions are reasonable

35. As in past authorizations in relation to the Justification Framework, the Minister indicates in this authorization that he seeks to delineate the boundaries of each class while authorizing a broad range of investigative activities within the parameters of each class. Therefore, for each class, he sets out i) the title of the class; ii) a definition of the class that includes a broad description of the types of acts in the class as well as the main legislative provisions under which the acts would otherwise be found to be unlawful; and iii) conclusions, in which he briefly outlines why it is necessary for CSIS to be able to commit, or direct the commission, of the acts within the particular class. I note that in his conclusions, the Minister makes it clear that he is relying on CSIS' information with respect to the types of otherwise unlawful acts that would be operationally useful.
36. The Minister also explains that when making his determination of the classes, he considered the overview of the classes prepared by CSIS; the Director's and the Deputy Minister's briefing notes, and CSIS' operational policies and procedures provided by the Director, including measures to reinforce the subsection 20.1(18) limitations and the respect of rights guaranteed by the *Charter* (s 20.1(22), *CSIS Act*).
37. The overview prepared by CSIS includes the following:

- a) a definition of the proposed class, which consists of a broad description of the class, a list of the main offences that would be included, as well as specific examples of activities that would constitute offences included in the class;
- b) a rationale for the class, which outlines the threat or object that investigations seek to address, as well as a general overview of why the offences would have to be committed in the context of an investigation;
- c) scenarios of operational use, which outlines situations where an otherwise illegal act could be committed, as well as additional specific examples describing situations where an act falling within the class has actually been committed; and
- d) a recommendation to the Minister to determine the class.

38. The Minister indicates that he adopts as an integral part of his own conclusions the definitions of each class and the rationales found in the overview prepared by CSIS. I have conducted my review on this basis.

39. On the basis of the information before him, the Minister concluded that the classes were reasonable in accordance with the legal requirements set out in subsection 20.1(3) of the *CSIS Act*. I find that the Minister's conclusions are reasonable.

40. The Minister's conclusions explain that the commission or the directing of the acts identified in the classes are rationally connected to CSIS' information and intelligence collection duties and functions. The rationale set out in the overview prepared by CSIS and relied on by the Minister explains in broad and intelligible strokes how committing offences can further CSIS' section 12 and section 16 investigations. In addition, the examples of specific acts that could, and have been, committed provide concrete situations that illustrate the link between the otherwise unlawful act, CSIS' investigation, and the threat being investigated.

41. As I have indicated in my 2023 decisions relating to the Justification Framework, the Minister is not required to provide an exhaustive list of offences included in a proposed class. What is required for the Minister's conclusions to be reasonable, however, is to demonstrate that a designated CSIS employee will be able to confirm that a contemplated act or omission actually falls within an approved class. It is therefore helpful to include examples of specific

offences when delineating a class. I find that the examples provided by the Minister bolster the understanding of the scope of the classes.

42. The Minister's conclusions, in addition to CSIS' overview of the classes adopted by the Minister, provide justification for why the classes are useful. The nature of the threat, or the object of the investigation, is explained, and the specific examples show that the commission of at least some of the otherwise unlawful acts is not merely a hypothetical occurrence.
43. I am also satisfied that the classes and the Minister's supporting conclusions are properly and clearly defined. They allow designated CSIS employees to have access to clear guidance with respect to what acts are included and excluded from the approved classes.
44. Further, I am satisfied that the Minister's conclusions are reasonable that *Charter* rights will be respected and the section 20.1(18) limitations will not be breached. The record is clear that designated CSIS employees must confirm there will be no infringement when the otherwise unlawful acts are carried out and shows that they receive mandatory training to ensure they can meet their responsibilities. Based on the information before him, the Minister was justified in being satisfied that measures in place, if applied appropriately, would lead to an implementation of the Justification Framework that respects the *Charter* and statutory limitations.

V. REMARKS

45. I would like to make three remarks to assist in the consideration and drafting of future determinations of classes of acts or omissions.

i) The responsibility of designated CSIS employees

46. The architecture of the *CSIS Act* is such that once the Intelligence Commissioner approves classes under the Justification Framework, CSIS employees are responsible to apply it in a manner that respects the rule of law. Misapplying the Justification Framework could lead designated employees, or persons directed by them, to commit an unlawful act that is not

legally justified – and therefore attract criminal liability. It could also mean that useful information collected by designated employees or directed persons acting covertly could be deemed to have been illegally collected and CSIS could be required to delete it.

47. Determining whether a proposed act falls within one of the approved classes is not the only decision made by a designated employee that is consequential to the legality of the proposed act. There are other elements a designated employee has to confirm for an otherwise unlawful act to be committed in accordance with the rule of law. In addition to the requirement that the acts not infringe on the *Charter* and respect the statutory limitations, as mentioned, a designated employee must confirm that they have reasonable grounds to believe that committing the otherwise unlawful act (s 20.1(11), *CSIS Act*) or directing another person to commit such an act (s 20.1(15), *CSIS Act*) is reasonable and proportional in the circumstances, having regard to the nature of the threat or the objective to be achieved, the nature of the act or omission and the reasonable availability of other means of proceeding.
48. Evidently, the Justification Framework places an extraordinary responsibility on each designated CSIS employee. This highlights the importance of the Minister's and the Intelligence Commissioner's role in ensuring clearly defined and understood classes of otherwise unlawful acts and omissions at the front end of the process, as well as the National Security and Intelligence Review Agency's (NSIRA) mandate to conduct *post-facto* reviews of CSIS activities.
49. I want to highlight the need to pay particular attention to a few specific legal considerations that are central to fulfilling this responsibility. In addition, I will highlight measures CSIS has in place to both guide employees in exercising this responsibility and verify that it is being applied in accordance with the rule of law.

a. Legal considerations in relation to the responsibility of designated CSIS employees

50. With respect to the statutory limitations set at in subsection 20.1(18) of the *CSIS Act*, it is useful to highlight part of a remark I made in my March 2023 decision (para 79), namely that some acts under the Justification Framework could, under certain conditions, devolve and

lead to a situation that is contrary to the statutory limitations. The designated employee therefore has the responsibility to evaluate the unknown, potential effects of a proposed act.

51. With respect to *Charter* rights, I have already stressed the importance of red lines.

Designated employees must be able to confirm that a proposed activity under the Justification Framework will not interfere with a reasonable expectation of privacy, which would infringe on rights protected under section 8 of the *Charter*. This can require a complex analysis. Indeed, it is a fact-specific and contextual exercise (see for example *R v McNeil*, 2009 SCC 1 at para 12). Adding to the complexity is the fact that defining a reasonable expectation of privacy is also an exercise of balance – between the right to be left alone by the state and the community’s interest in advancing the protection of the community (*R v Bykovets*, 2024 SCC 6 at para 71). As a result, a particular act committed in the past that raised no issues relating to privacy interests could, in different circumstances, give rise to an unreasonable search or seizure. The impact of specific circumstances could also apply to rights protected by other sections of the *Charter*.

52. Finally, in relation to determining whether an act is reasonable and proportional in the circumstances, a designated employee must conduct a balancing exercise that incorporates a legal threshold (reasonable grounds to believe), as well as concepts that are to be legally applied (reasonable and proportional) (s 20.1(11) and (15), *CSIS Act*). This can be complex, especially considering the impact of an otherwise illegal activity.

53. Indeed, designated employees are responsible for evaluating the impact of the proposed act, and therefore giving proper consideration to the interests that will be impacted. Not all interests will be given the same importance in the balancing. Some acts may have very minimal impact beyond an individual or group under investigation (for example, [...]). The interests impacted by other acts could be collective in nature (for example, [...]), and be aimed at fundamental Canadian institutions or the values they represent. Acts could also have an impact on a specific individual (for example [...]), in which case, the designated employee would effectively be deciding that the Government of Canada was legally justified in committing an offence where the victim is a Canadian.

54. In summary, the extraordinary responsibility of determining whether an otherwise illegal act can be committed is accompanied by having to balance the interests that may require a sophisticated understanding of the applicable legal concepts.

b. Measures in place to guide designated employees

55. Given the high level of responsibility placed on designated CSIS employees applying the Justification Framework, as well as the complexity in applying it, it is imperative for them to fully understand their role and responsibilities, and have the necessary information and resources to meet those responsibilities. In that regard, the materials provided in the record highlight the importance of employee training and how all actions and decisions associated with using the Justification Framework must be reported and conducted within the limits of the *CSIS Act*, Ministerial Directions and CSIS policies.

56. Prior to being designated under the Justification Framework, designated CSIS employees must successfully complete mandatory training comprised of e-modules and in-person workshops. A mandatory annual recertification e-training must also be successfully completed by employees seeking to maintain their designation. The employees' understanding of the Justification Framework is evaluated through practical exercises and scenarios, which, having reviewed the examples provided in the record, I find are useful to understand the scope and limitations of the eight classes as well as the proper application of complex legal requirements. The importance placed on employee training by CSIS is clearly stated in their policy and reflected in the training materials provided for my review. Given the complexity of the decisions they must make, I am of the view that it is at the core of the application of the Justification Framework.

57. In addition to training, reporting helps to ensure that the Justification Framework is being applied in accordance with the rule of law by ensuring that there is an opportunity to review decisions to use it. Whenever an act is committed pursuant to the Justification Framework, a designated employee must submit a written report to a designated senior employee or the

Director describing the act (s 20.1(23), *CSIS Act*). CSIS subsequently provides a copy of the report to NSIRA (s 20.1(26)(c), *CSIS Act*).

58. Finally, CSIS operational policies set out the procedures to be followed for the Justification Framework to be used and help guide designated employees in their decision making. The policies set out that in some cases, acts that would fall within the Justification Framework are part of an operational plan that requires approval from designated senior officials. The policies also require a designated employee to prepare a “Reasonable and Proportionality Statement” prior to conducting or directing the commission of an otherwise unlawful act, and sets out elements that must be considered in the statement, namely i) the nature of the threat (section 12) or the objective (section 16), as applicable; ii) the impact of committing or directing the illegal act or omission; iii) an assessment of the threat or objective versus the impact of committing the act; iv) the rational link between the proposed activity and the expected results; v) other options considered; vi) the impact of not proceeding with the otherwise illegal activity.

c. The potential for the Minister to consider other factors in his conclusions

59. Section 20.1(3) states that the Minister may determine a class of acts or omissions if he concludes that the commission of those acts or omissions is reasonable “having regard to” (*compte tenu*) two factors: CSIS’ information and intelligence collection duties and functions, and any threats to the security of Canada that may be the object of information and intelligence collection activities (s 12) or any objectives to be achieved by such activities (s 16).

60. However, the extraordinary responsibility given to designated CSIS employees highlights the importance of the measures CSIS has in place – training, reporting, policies – to ensure that the Justification Framework will be applied in a way that respects the rule of law. In my view, when the Minister issues an authorization setting out the classes of acts or omissions, it is open to the Minister to also “have regard” to how the Justification Framework will be applied. Indeed, the Minister may not want to authorize classes if he is not confident that,

once the classes are approved by the Intelligence Commissioner, the Justification Framework would be applied in a way that respects the rule of law. It follows that it could be a factor to be considered by the Minister in his conclusions when determining whether the classes of acts or omissions are reasonable. Similarly, this consideration, or the absence of it, in ministerial conclusions could factor into the Intelligence Commissioner's review.

ii) Impact of recent judicial decision

61. I note that in one of the scenarios of operational use set out in the record, an otherwise unlawful act ([...]). I note that the recent Supreme Court of Canada decision in *R v Bykovets*, 2024 SCC 6, rendered after the Minister's authorization, may require CSIS to review certain warrantless activities to ensure they are being conducted in accordance with the rule of law.

iii) Additional information for the Minister

62. The record contains a statistical overview of the use of the Justification Framework for 2022–23, including the number of emergency designations (an imminent threat or a time-sensitive operation); authorizations issued by senior designated employees from active source operations; and occurrences when designated employees directed individuals or when they committed acts or omissions themselves.
63. The record also includes a list, with a brief description, of every act committed by designated CSIS employees pursuant to the Justification Framework. I consider the seriousness of the illegality of all of these acts to be minimal in nature. However, there is no description of the acts committed by persons directed by designated employees. A complete picture of how the Justification Framework is being used should be provided to the Minister.

64. Likewise, it could be helpful for the Minister, and myself, for the record to include additional information on how CSIS ensures that persons directed by designated CSIS employees act in accordance with the rule of law.
65. Finally, I note that the activities falling within the approved classes seem to constitute only “acts” and not “omissions”, and raise for consideration whether additional details in that regard would be beneficial to designated CSIS employees implementing the Justification Framework.

VI. CONCLUSIONS

66. Based on my review of the record submitted, I find that the Minister’s conclusions on which Classes 1 to 8 are determined are reasonable.
67. In accordance with paragraph 20(1)(a) of the *IC Act*, I approve the Minister’s Authorization of Class 1 to 8 dated February 12, 2024 for a period of one year from the date of this decision.
68. As prescribed in section 21 of the *IC Act*, a copy of this decision will be provided to the National Security and Intelligence Review Agency for the purpose of assisting it in fulfilling its mandate under paragraphs 8(1)(a) to (c) of the *National Security and Intelligence Review Agency Act*, SC 2019, c 13, s 2.

March 11, 2024

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner