Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

National Security and Intelligence Review Agency | **Office de surveillance des activités en matière de sécurité nationale et de renseignement**

Review of the Canadian Security Intelligence Service's Use of the Justification Framework

NSIRA // Review 24-05

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Table of Contents

Executive Summary ii

List of Abbreviations iii

I. Introduction 1

Authority 1

Scope 1

Methodology 1

Review Statements 2

II. Background 2

Origins of the CSIS Justification Framework 2

Classes of Acts or Omissions 4

Designated Employees 4

Designated Senior Employees 5

Commission of Acts or Omissions 6

Direction of Acts or Omissions 6

Reporting Requirements 6

III. Findings, Analysis, and Recommendations 7

Justification Framework Limitations 7

Justification for Acts or Omissions 8

Commission of Acts or Omissions without Designation 11

Direction of Acts or Omissions without Authorization 12

Transparency and Accountability 12

IV. Conclusion 15

Annex A. Justification Framework Process 16

Annex B. Findings and Recommendations 17

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Executive Summary

Section 20.1 of the *Canadian Security Intelligence Service Act* ("CSIS Act") provides a limited legal framework through which certain Canadian Security Intelligence Service (CSIS) employees and other persons acting under their direction may commit acts or omissions that would otherwise constitute offences (A/O) when collecting information or intelligence pursuant to the CSIS mandate. Otherwise known as the justification framework (JF), it is designed to ensure that CSIS operations remain within the bounds of the rule of law.

In conducting this review, NSIRA focused on CSIS's use of the JF in operations. NSIRA reviewed a sample of operational reporting involving the JF in 2022 and 2023 and found that CSIS operations involving use of the JF respected statutory limitations.

However, NSIRA also found several instances where CSIS's use of the JF may not have been in compliance with the CSIS Act, ranging from employees committing A/O without proper designation to direction of A/O without proper authorization. Other compliance issues pertained to reporting requirements pursuant to the CSIS Act.

A key requirement of the JF is for employees committing or directing A/O to believe that the activity is reasonable and proportional when collecting information or intelligence related to the CSIS mandate. NSIRA identified multiple gaps in the structure and substance of documentation of the reasonableness and proportionality considerations of employees. This indicates that CSIS employees sometimes lacked a clear understanding of pertinent policy requirements related to conducting a detailed assessment. In addition, NSIRA identified an absence of thorough internal oversight and guidance. To this effect, NSIRA recommends that CSIS improve internal guidance on JF issues and conduct the necessary oversight and quality assurance to ensure compliance.

The JF is an important power enabling CSIS to deliver on its mandate to collect intelligence related to threats to the security of Canada or foreign intelligence within Canada. CSIS has a duty to ensure that all of its operations respect the rule of law, even more so when those operations require activity that would otherwise be considered illegal.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

List of Abbreviations

A/O	Acts or omissions that would otherwise constitute offences
CSIS	Canadian Security Intelligence Service
JF	Justification Framework
NSIRA	National Security and Intelligence Review Agency

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

I. Introduction

Authority

1. This review was conducted under the authority of paragraphs 8(1)(a) and 8(1)(b) of the *National Security and Intelligence Review Agency Act* ("NSIRA Act").[1]

Scope

2. The National Security and Intelligence Review Agency (NSIRA) reviewed Canadian Security Intelligence Service (CSIS) operations involving the use of section 20.1 of the CSIS Act between January 1, 2022 and December 31, 2023.
3. NSIRA evaluated CSIS's compliance with the law, including the reasonableness and necessity of CSIS's conduct of acts or omissions that would otherwise constitute offences (A/O). NSIRA focused on operations in which CSIS considered that the activity met the threshold of requiring use of the justification framework (JF). This did not include operations in which the JF was not invoked.
4. NSIRA also reviewed the role Public Safety Canada plays in facilitating the annual determination of classes of A/O and the designation of CSIS employees by the Minister of Public Safety.

Methodology

5. NSIRA used a variety of methods to meet this review's objectives including, but not limited to, information requests, briefings from subject matter experts, and documentary analysis.
6. NSIRA focused its research on specific CSIS operations involving the use of the JF, selecting a sample of # operational files for closer review. This sample was drawn from information CSIS is required to provide to NSIRA regarding its use of the JF pursuant to section 20.1(26) of the CSIS Act. Following which, NSIRA selected individual files for closer review based on a range of factors, such as the class(es) of A/O being used, the threat being investigated, and the CSIS region or branch conducting the operation. At the outset of this review NSIRA sought access to a larger sample set, however, due to the comingling

15(1)(d)

[1] SC 2019, c 13 [NSIRA Act].

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

of data described below resulting in lengthy delays in accessing the required information, NSIRA reduced the sample size to facilitate completion of the Review.

Review Statements

7. The NSIRA Act grants NSIRA rights of timely access to any information in the possession or under the control of a department (except for Cabinet confidences) and to receive from the department any documents and explanations NSIRA deems necessary. NSIRA monitors cooperation with access requests, including the completeness and accuracy of disclosures, which inform its overall assessment of a department's responsiveness in each review.[2]

8. Much of the information documenting CSIS's use of the JF is located in the same operational reports which also contain information identifying its human sources. NSIRA determined that it did not require access to this identifying information for the purposes of this review. Prior to providing access to NSIRA, CSIS redacted information at its discretion. This process required CSIS to devote what it characterized as thousands of hours to process these reports and resulted in considerable delays before NSIRA could access information it required. Accordingly, CSIS did not meet NSIRA's expectations for responsiveness in this review.

9. Public Safety Canada met NSIRA's expectations for responsiveness during this review.

II. Background

Origins of the CSIS Justification Framework

10. In 2019, Parliament passed the *National Security Act, 2017*, which amended the *Canadian Security Intelligence Service Act* ("CSIS Act") with section 20.1.[3] Colloquially known as the JF, this section established a limited legal justification for certain CSIS employees, and others subject to their direction, to commit A/O when engaged in information and intelligence collection operations pursuant to CSIS's mandate. See Annex A for a diagram explaining the major elements of the JF, as described below.

11. CSIS's information and intelligence collection mandates are found at sections 12 and 16 of the CSIS Act. Section 12 relates to CSIS's investigations of threats to the security of

[2] NSIRA's "Expectations for Responsiveness in Reviews" are online at https://nsira-ossnr.gc.ca.

[3] RSC 1985, c C-23 [CSIS Act] s. 20.1.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Canada. Pursuant to section 16, CSIS may also assist the Ministers of National Defence or Foreign Affairs with the collection of foreign intelligence from within Canada.[4]

12. Following amendment in 2019, the CSIS Act expressly recognizes that:

> It is in the public interest to ensure that employees effectively carry out the Service's information and intelligence collection duties and functions, including by engaging in covert activities, in accordance with the rule of law and, to that end, to expressly recognize in law a limited justification for designated employees acting in good faith and persons acting under their direction to commit acts or omissions that would otherwise constitute offences.[5]

13. Prior to 2019, CSIS operated under the belief that illegal activity conducted by employees or individuals directed by them, such as human sources, was legally covered by the doctrine of Crown immunity. In a 2014 review, NSIRA's predecessor, the Security Intelligence Review Committee raised concerns related to the legality of CSIS operations and, in particular, potential violations of the United Nations Al-Qaida and Taliban Regulations in intelligence collection operations.[6] In 2015, the Committee recommended that CSIS seek legal clarification on whether CSIS employees and CSIS human sources were afforded protection under the common law rule of Crown immunity with regard to terrorism-related offences of the *Criminal Code*.[7]

14. In 2020, the Federal Court, having taken notice of these reviews, was critical of CSIS's reliance on Crown immunity in its decision regarding the validity of several warrant applications predating the JF. The Court found that CSIS breached its duty of candour by not disclosing that information may have been collected illegally as it did not benefit from Crown immunity which had by then eroded. In particular, this illegality involved conduct by CSIS or human sources acting at its direction that was likely contrary to the anti-terrorism provisions of the Criminal Code.[8]

15. These reviews and Court decisions, in part, helped to identify larger issues related to CSIS's reliance on Crown immunity to provide legal justification for A/O in pursuit of its mandate. Ultimately, Parliament amended the CSIS Act to explicitly provide CSIS with a legal framework to conduct A/O.

15(1)(d) [4] In 2022 and 2023, CSIS's use of the JF [redacted]

[5] CSIS Act, ss. 20.1(2).

[6] Security and Intelligence Review Committee Review of CSIS's relationship with the Department of Foreign Affairs, Trade and Development (2014-07).

[7] Security and Intelligence Review Committee Review of CSIS's investigation of Canadian "foreign fighters" (2015-09).

[8] RSC 1985, c C-46 [*Criminal Code*].

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Classes of Acts or Omissions

16. Before CSIS can commit or direct others to commit A/O, the Minister of Public Safety must, at least once every year, determine classes of A/O that CSIS employees, and those under their direction, may be justified in committing. To date, CSIS has only publicly acknowledged one class related to terrorism offences. All other classes remain classified.

17. The Minister's annual determination is managed by CSIS and Public Safety Canada. CSIS consults internally to determine if classes remain appropriate and meet operational needs or if modifications or entirely new classes are required. New or amended legislation, or operational developments, including changing intelligence requirements in response to a fluid threat environment, may require new classes or modifications to existing classes. When applying to the Minister, CSIS identifies and describes the classes of A/O it believes may be required when collecting information or intelligence. CSIS also provides specific examples to assist the Minister in establishing the classes. The Deputy Minister of Public Safety, supported by departmental staff, provides advice to the Minister based on CSIS's submission and regular consultation with CSIS.

18. The Minister's order determining classes of A/O is subject to approval by the Intelligence Commissioner, who ensures that the basis upon which the Minister's decision was made was reasonable.

19. In July 2019, in his first order, the Minister determined seven classes of A/O. However, the Commissioner did not approve any of the classes as he found that the Minister had not made conclusions supporting his determination of the classes, which form the basis of the Commissioner's approval. In September of that year, the Minister reissued his determination, this time including the required conclusions. The Commissioner approved six of the seven classes, but did not approve the seventh class as he found that the Minister's conclusions for this class "lacked justification and intelligibility with respect to some of the acts or omissions falling within the class." The Commissioner ultimately approved the Minister's determination of the seven classes of A/O in October 2020 and November 2021.

20. In July 2022, an eighth class was added, distinguishing certain A/O from broader terrorism offences. Following amendments in response to concern raised by the Intelligence Commissioner, CSIS has operated under largely the same eight classes since June 2023.

Designated Employees

21. CSIS employees using the JF must be personally designated by the Minister, on the recommendation of the Director. The Minister's designation of employees is valid for up

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

to one year. Unlike the Minister's determination of classes, the designation of CSIS employees is not subject to review or approval by the Intelligence Commissioner.

22. Employees are identified to the Minister by a unique employee number rather than by name. Although the Minister may designate employees as required and on an *ad hoc* basis, CSIS has implemented a cycle for designations that takes place twice a year.

23. The designation of CSIS employees is coordinated internally by the policy centre responsible for the JF. CSIS employees must first complete internal training requirements prior to becoming designated. Training involves successful completion of self-directed and in-person courses that apprise employees about the background and requirements for the JF, the classes of offences, policies and procedures governing use of the JF, special considerations and limitations for employees when invoking the JF, and the concepts of reasonableness and proportionality. Once complete, employees attest to understanding their roles and responsibilities prior to their designation.

24. In practice following approval by the Director, CSIS sends the designation package to Public Safety Canada where it is reviewed by departmental staff. The CSIS Director's application is provided to the Minister, along with a recommendation from the Deputy Minister for decision. In 2022, the Minister designated [#] employees and in 2023 this number decreased to [#].

Designated Senior Employees

25. The Minister may also designate senior employees under the JF.[9] These employees are responsible for authorizing a designated employee to direct another person to commit A/O and for receiving written reports describing the commission or direction of A/O.[10] Senior employees must also complete internal training prior to receiving their designation, as well as annual refresher training. Unlike designated employees, senior employees do not require annual re-designation and their status remains in effect until rescinded. In 2022, there were [#] senior employees designated by the Minister, which increased to [#] in 2023.

---

[9] CSIS policy uses the term "senior designated employee" to describe these employees. However, the CSIS Act refers to designated senior employees. NSIRA will use the language from the CSIS Act throughout this report.

[10] The CSIS Act permits the Director or a designated senior employee to authorize direction, however, in the files reviewed by NSIRA, authorizations to direct were only granted by senior employees.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Commission of Acts or Omissions

26. For a CSIS employee to commit A/O, they must be designated by the Minister, and be engaged, in good faith, in an information and intelligence collection activity in relation to the CSIS mandate. They must also believe on reasonable grounds that the A/O they will commit are reasonable and proportional in the circumstances.

Direction of Acts or Omissions

27. A designated employee may also direct another person, other than a CSIS employee, to commit A/O. To do so, they must first meet the criteria required to commit A/O. Unlike commission, a designated employee directing another person to commit A/O must also be authorized by a designated senior employee. Additionally, the person being directed must have reasonable grounds to believe that the person giving the direction has the authority to do so.

28. Authorization for a designated employee to direct another person to commit A/O is valid for up to one year and is generally requested via CSIS's standard operational approval process. When approved in advance, a request for authorization must describe the A/O expected within the coming year, and ensure that they are related to an approved class. The designated employee must also establish the grounds upon which they believe that the anticipated A/O will be reasonable and proportional.

29. Once authorization to direct is received, a designated employee has the authority to direct another person to commit A/O, as long as the A/O remain reasonable and proportional at the time of direction. Any change in the A/O being directed or in the circumstances affecting the justification for the A/O may require a new authorization.

Reporting Requirements

30. The CSIS Act requires that a designated employee who commits or directs another person to commit A/O must submit a written report to the Director or a designated senior employee describing the A/O as soon as possible after doing so. CSIS policy requires that these reports are included in relevant operational reporting and sent to a designated senior employee and the policy centre responsible for the JF for awareness, tracking and external reporting purposes.

31. Separately, the Minister is required, every year, to publish or otherwise make available to the public certain information and statistics about how CSIS used the JF in the previous year. CSIS must also notify NSIRA as soon as the circumstances permit after an emergency

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

designation is made, an authorization to direct is given or a report of commission or direction of A/O is submitted.

III. Findings, Analysis, and Recommendations

Justification Framework Limitations

Finding 1. NSIRA found that CSIS complied with the limitations on the use of the justification framework in all operations reviewed.

32. The CSIS Act contains important limitations restricting CSIS's use of the framework, providing guardrails against certain activity which is not authorized, under any circumstances. Stated generally, these limitations prohibit CSIS from:

- causing, intentionally or by criminal negligence, death or bodily harm to an individual;
- wilfully attempting in any manner to obstruct, pervert or defeat the course of justice;
- violating the sexual integrity of an individual;
- subjecting an individual to torture or cruel, inhuman or degrading treatment or punishment;
- detaining an individual;
- causing the loss or serious damage to property, if doing so would endanger the safety of an individual;
- committing offences specified in a direction issued by the Minister;
- circumventing the requirement to obtain a warrant from the Federal Court; or
- infringing a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms*.

33. These limitations are further highlighted in CSIS Policy with an additional requirement that employees invoking the JF include the following statement in all operational reporting documenting the use of the JF:

> I confirm I am a designated employee as per section 20.1 of the CSIS Act. I confirm that I have considered the rights and freedoms guaranteed by the Charter, and the s.20.1(18) Limitations.

34. NSIRA reviewed CSIS reporting for [#] operations in which the JF was invoked between 2022 and 2023 (inclusive), and observed no indication that CSIS's use of the JF contravened any of the CSIS Act limitations.

15(1)(d)

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Justification for Acts or Omissions

Finding 2. NSIRA found that, in # operations reviewed, CSIS employees insufficiently documented the reasonableness and proportionality of the commission or direction of acts or omissions that would otherwise constitute offences, contrary to CSIS policy.

35. The CSIS Act requires that a designated employee committing or directing A/O has reasonable grounds to believe that they are reasonable and proportional in the circumstances. This employee must take into account certain minimal considerations to justify the conduct of A/O. These include the nature of the threat or objective, the nature of the A/O and the reasonable availability of other means for performing the information and intelligence collection activity.

36. CSIS policy requires that employees document their justification for A/O in a reasonableness and proportionality statement. CSIS policy expands on the three criteria found in the CSIS Act, requiring employees to consider six elements in their statement including:

    - What is the nature of the threat?
    - What is the negative impact of committing the A/O?
    - Given the threat and impact, is the activity reasonable?
    - What is the rational link between the A/O and the expected results?
    - What other options have been considered?
    - What is the impact of not proceeding with the A/O?

37. Training materials reviewed stress that reasonableness and proportionality statements are individual, based on the personal belief of the employee, and must address at least the six elements identified in policy. Scenarios included in relevant training materials dealt with elements of crafting robust statements, including examples of required documentation.

38. Sufficient consideration of the nature of the threat being investigated, the nature of the A/O and the reasonable availability of alternatives to using the JF all factor into the justification for A/O. Personal belief that A/O were justified in the circumstances is a key factor for CSIS employees to ensure that the JF is appropriately applied. When these factors are overlooked or considered insufficiently, the grounds upon which CSIS builds its justification may be called into question. This may result in the operational activity losing the legal protection of the JF, exposing CSIS employees and others under their direction to unnecessary legal risk.

39. NSIRA reviewed # human source operations against the CSIS Act requirements using the justification documented for each file. In # of these operations, NSIRA found notable

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

issues with the employee reasonableness and proportionality statements. Some files included issues with one, two or all three of the categories discussed below.

Nature of the Threat

40. In [#] operations, employee statements lacked a clear description of the nature of the threat requiring use of the JF. In some, the statement did not describe the nature of the threat at all. In others, employees stated that A/O were justified because CSIS was investigating the activities of a certain individual or group, or that the investigation was of a high priority, thereby posing a threat to the security of Canada. A clear and concise description of the nature of the specific threat necessitating CSIS to conduct A/O to carry out its mandate is foundational in establishing the justification for A/O. On its own, the fact that CSIS has an open investigation is insufficient as it does not establish or support the justification for specific A/O required in the circumstances of that investigation.

Nature of the Acts or Omissions

41. In [#] operations, employee statements lacked a clear description of the nature of the A/O, specifically their negative impact. [redacted] the designated employee only described the positive impact of committing the activity (i.e. facilitating CSIS's access to information), while [redacted], the negative impact of committing the A/O was not addressed. Assessing the impact of A/O to individuals, or society as a whole, is an important consideration establishing the justification for A/O in the circumstances.

Consideration of Alternatives

42. In [#] operations, employee statements lacked a sufficient description of the consideration of alternatives to A/O. In some cases, employees neglected to document consideration of any alternatives. In others, employees stated that they had considered alternatives or that no alternatives were available without providing any concrete examples or further explanation. Consideration of alternatives to A/O does not necessitate exhaustion of all alternatives. However, as part of the justification for A/O, CSIS should be able to demonstrate, with concrete examples, that reasonable alternatives to conducting A/O have at least been considered or attempted, when appropriate, prior to using the JF.

Other Issues

43. Finally, in [#] operations, NSIRA observed indications of duplicate language from reasonableness and proportionality statements, in whole or in part, across documents within operational files. In one notable example, the statement cited the [redacted] from the one being directed to commit A/O, indicating reuse of

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

statements between operations. Although there may be a reasonable basis for employees to reuse language if the circumstances of an operation have not changed, a strong, defensible and personal justification for A/O is an important element underlying the legal protections of the JF.

44. Each year, CSIS reports [#] of instances where the JF is used. The JF policy centre is the unit responsible for identifying deficiencies such as those noted above. The unit, [redacted], is also responsible for the coordination of the annual determination of classes of A/O and designation of employees, updating JF policies and procedures, preparing and delivering JF-focused training, and satisfying internal and external briefing requirements. These critical processes occupy a significant portion of this employee's time and effort on an annual cycle. While NSIRA observed instances where issues with reasonableness and proportionality statements were identified by the JF policy centre and subsequently addressed prior to the conduct of operational activity, oversight and quality control of these statements and other JF documentation requirements were a secondary responsibility of this employee.

45. The impact of these resource limitations on the overall use of the JF within CSIS were noted in a 2023 internal CSIS evaluation. This evaluation identified that the JF policy centre was integral to the functioning of the JF, but that staffing challenges had negative impacts on the use of the program. Furthermore, it noted that despite the publication of updated policy and procedures specific to the JF, operational personnel continued to request greater advice and guidance when using the JF. The evaluation also found that the unit's "compliance work is reactive and ad hoc rather than planned and proactive, and there is no back-up available to provide advice and support when staff members are not available..." Following the publication of this evaluation, staffing levels remained unchanged within the JF policy centre.

46. Improving and enhancing internal guidance and oversight is required in order ensure adherence to statutory requirements. Many of the deficiencies in reasonableness and proportionality statements noted above can be attributed to confusion or a lack of understanding of the requirements and the consequences of not meeting them. To this effect, it is pivotal to ensure that employees have access to and are supported by internal subject matter experts that may provide guidance in situations where there is uncertainty. Moreover, this function may serve to provide the visibility needed to ensure that identified gaps are integrated and addressed in future training such that some of the issues may be resolved prior to their materialization.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Recommendation 1. NSIRA recommends that CSIS improve and enhance internal guidance, oversight, and quality assurance of documentation supporting employee use of the justification framework. This function should be resourced in a manner commensurate with the importance and scale of the justification framework to CSIS operations, in order to ensure compliance with the CSIS Act and internal policy requirements.

Commission of Acts or Omissions without Designation

Finding 3. NSIRA found that CSIS may not have been in compliance with subsection 20.1(11) of the CSIS Act when [#] employees committed acts or omissions that would otherwise constitute offences while not designated by the Minister.

47. The CSIS Act requires that all employees committing A/O, including those engaged in covert activities, be designated by the Minister and form reasonable grounds upon which they believe that A/O are reasonable and proportional in the circumstances. Employees not meeting these statutory requirements may not benefit from the legal protections of the JF and could result in CSIS undertaking higher levels of legal risk.

48. [redacted] 2023, [#] CSIS employees, [redacted] committed A/O under class [redacted] For all [#] the reasonableness and proportionality statements were written by another employee, rather than by the employee(s) committing the A/O.

49. Despite the fact that CSIS employees committed the A/O in question, because [redacted] CSIS considered them to be in a "supporting role" in the operation which did not necessitate their being designated by the Minister. However, the CSIS Act provides no such exclusion to the designation requirement. In addition to not seeking designation of these employees, they were not required to document the grounds upon which they believed in the reasonableness and proportionality of the A/O in the circumstances.

50. Designation of employees by the Minister is a legal requirement pursuant to the CSIS Act. CSIS employees must also personally believe that A/O were reasonable and proportional in the circumstances. Furthermore, while documentation of reasonableness and proportionality statements is a policy, rather than statutory requirement, an employee's belief in the reasonableness and proportionality of the A/O cannot be established by others.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Direction of Acts or Omissions without Authorization

Finding 4. NSIRA found that CSIS may not have been in compliance with subsections 20.1(12) and (15) of the CSIS Act when [#] employees directed acts or omissions that would otherwise constitute offences absent authorization from the Director or a designated senior employee.

51. The CSIS Act requires that designated employees obtain the authorization of a senior employee to direct another person to commit A/O. CSIS policy and procedures require this authorization to be documented in relevant operational reporting. NSIRA observed [#] cases where this requirement was not met.

52. The first was in [redacted] 2022, when a designated employee directed a human source to commit A/O under class [redacted] Senior employee authorization for this employee to direct the source had expired prior to the direction being given and was not renewed until the following month.

53. The second, involved multiple instances from [redacted] 2023, when a designated employee directed a human source to commit A/O under class [redacted]. However, the employee was not authorized by a senior employee to direct this [redacted] to commit A/O.

Transparency and Accountability

54. Transparency and accountability are important mechanisms to protect against the risk of excessive or unreasonable use of powers such as the JF. They contribute to striking a balance between the needs of the state, such as in matters of national security, while upholding the rule of law. As it relates to the JF, transparency and accountability are primarily addressed through internal and public reporting requirements as well as independent, external review by NSIRA.

Within CSIS

Finding 5. NSIRA found that CSIS may not have been in compliance with subsection 20.1(23) of the CSIS Act in [#] operations when employees did not report in writing to the Director or a designated senior employee following the commission or direction of [#] acts or omissions that would otherwise constitute offences.

55. The CSIS Act requires that CSIS employees submit a written report to the Director or a designated senior employee describing the A/O as soon as the circumstances permit after they occur.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

56. CSIS policy and procedures require both commission and direction of A/O to be documented by the responsible employee in the relevant operational report. Although the relevant report may be different depending on the circumstances of the operation, the fact that all instances of CSIS's use of A/O in operations are accurately reported is paramount.

57. CSIS policy also requires that reports documenting use of the JF be sent to the JF policy centre. The policy centre is responsible to compile information related to use of the JF which is subsequently used to satisfy CSIS's requirement to report to NSIRA as well as the Minister's requirement to report publicly.

58. In [#] operations reviewed, NSIRA found [#] instances where CSIS failed to submit written reports of commission or direction of A/O. In some instances, CSIS reported one or the other, when both should have been reported. In others, CSIS failed to report either.

59. Written reports describing A/O committed or directed by CSIS employees are not only a requirement of the CSIS Act, but they also form the basis of the information required to satisfy other accountability mechanisms, as discussed below.

To NSIRA

Finding 6. NSIRA found that CSIS may not have been in compliance with subsection 20.1(26)(c) of the CSIS Act when it did not notify NSIRA of all reports of commission or direction of acts or omissions that would otherwise constitute offences.

60. CSIS is required to notify NSIRA about multiple operational activities, including its use of the JF.[11] Reporting requirements, such as these, are intended to provide NSIRA with information and visibility to be able to verify and review these activities. These requirements help to ensure that CSIS remains fully accountable to Canadians for its activities.

61. During Parliament's consideration of amendments to the CSIS Act, CSIS advocated for the JF, in part, by explaining that these powers would be subject to "measures to ensure this authority is exercised in a manner that is reasonable, proportional, transparent and accountable, including robust review by... [NSIRA]." Similarly, the Department of Justice Canada assured Parliament and Canadians that "as with other powers under the CSIS Act, the justification measures are subject to review by... NSIRA and to the power of... NSIRA to report on the activities taken under the measures."

[11] In addition to JF requirements, these include: ministerial direction to CSIS, the Director's report to the Minister, the CSIS dataset regime, threat reduction measures, cooperation arrangements, disclosure of information and unlawful conduct (other than that authorized by the JF).

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

62. It is clear that Parliament intended to have greater scrutiny of the JF regime through NSIRA's review. Within the CSIS Act this intent is clear with requirements for CSIS to notify NSIRA of the following information related to its use of the JF:

    - an emergency employee designation is made under subsection 20.1(8);
    - an authorization to direct A/O under subsection 20.1(12) is given; and
    - a written report is submitted under subsection 20.1(23) following the direction or commission of A/O.

63. CSIS policy states that "employees must ensure all activities pertaining to the use of the [JF] are documented and distributed according to the requirements established in" relevant CSIS policy and procedures. The JF policy centre then compiles information about these reports into quarterly notifications to NSIRA.[12]

64. In NSIRA's sample of [#] operational files, NSIRA identified inaccuracies with the information provided by CSIS for 2022 and 2023. CSIS did not notify NSIRA of [#] reports of direction of A/O in 2022 and [#] in 2023. Similarly, CSIS did not notify NSIRA of [#] reports of commission of A/O in 2023. Of these examples, some were the result of CSIS employees who both committed and directed a source to commit A/O but only reported the event as one or the other. Other examples were instances where CSIS employees did not report the direction or commission in line with CSIS policy or the CSIS Act.

To the public

Finding 7. NSIRA found that the Minister of Public Safety may not have been in compliance with subsection 20.1(24) of the CSIS Act when they did not annually publish or make available a report in respect of CSIS's use of the justification framework for 2019, 2020, 2021 or 2022.

65. The CSIS Act requires the Minister of Public Safety to "every year, publish or otherwise make available to the public a report in respect of the previous year..." describing CSIS's use of the JF. Typically, requirements such as this would be satisfied by the Department of Public Safety and/or CSIS, on behalf of the Minister.

66. Prior to 2024, there were no annual public reports describing CSIS's use of the JF. In March 2024, CSIS began publishing information satisfying this requirement in its public report for 2023. This report included information about CSIS's use of the JF from 2019 until 2023. Although CSIS has begun releasing information on an annual basis on behalf of the

[12] It should be noted that these notifications do not include the content of the reports but rather data about the reports, such as report numbers, operation codename, classes of A/O involved, date the A/O was committed or directed, and the CSIS region in which the operation took place.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Minister, the retroactive release of this information in 2024 did not meet the requirement to report "every year" as required by the CSIS Act.

67. Greater emphasis on accurate reporting internally at CSIS may bolster accountability and transparency for CSIS's use of the JF not only to NSIRA and the Minister but to the public writ large.

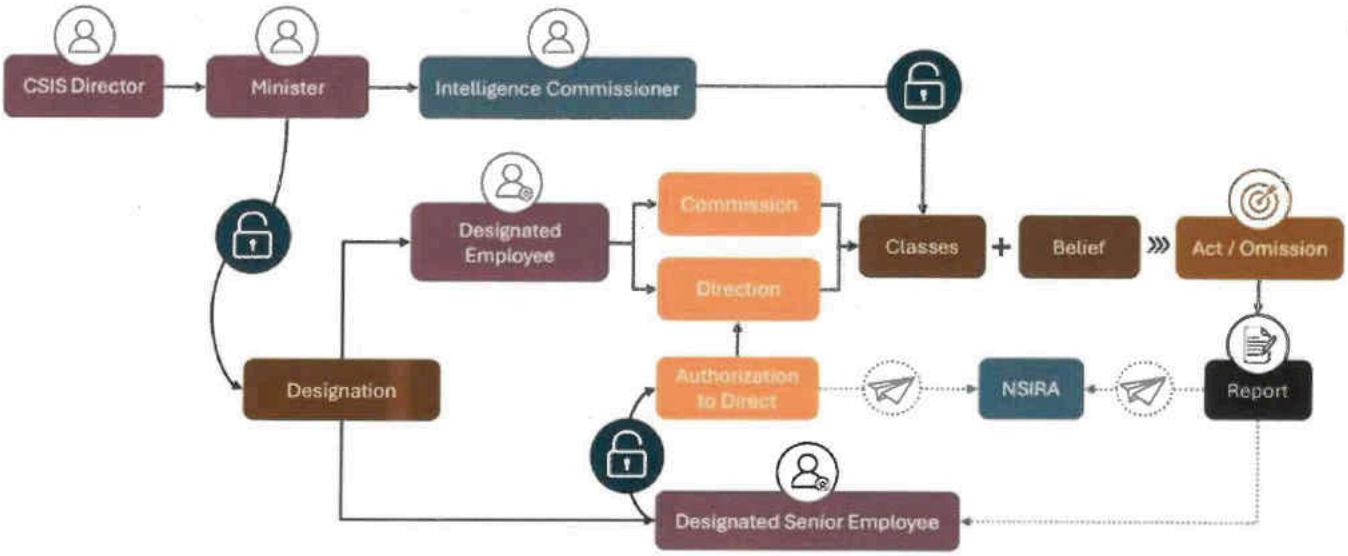
IV. Conclusion

68. Section 20.1 of the CSIS Act provides CSIS with a legal framework under which select employees may commit or direct others to commit A/O when collecting information or intelligence related to its mandate. It is designed to ensure that CSIS operations do not contravene the law. Given the gravity and potential for misuse, this authority comes with significant limitations and requirements designed to ensure there are legal guardrails for CSIS operations.

69. Based on the limited sample set examined, NSIRA found multiple instances where CSIS's use of the JF may not have been in compliance with the CSIS Act. The issues and gaps identified in this report warrant an institutional resolve to ensure operations remain within the bounds of the rule of law and that requirements for public accountability are met.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Annex A. Justification Framework Process



Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Annex B. Findings and Recommendations

NSIRA made the following findings and recommendations in this review:

Justification Framework Limitations

Finding 1. NSIRA found that CSIS complied with the limitations on the use of the justification framework in all operations reviewed.

Justification for Acts or Omissions

Finding 2. NSIRA found that, in [#] operations reviewed, CSIS employees insufficiently documented the reasonableness and proportionality of the commission or direction of acts or omissions that would otherwise constitute offences, contrary to CSIS policy.

Recommendation 1. NSIRA recommends that CSIS improve and enhance internal guidance, oversight, and quality assurance of documentation supporting employee use of the justification framework. This function should be resourced in a manner commensurate with the importance and scale of the justification framework to CSIS operations, in order to ensure compliance with the CSIS Act and internal policy requirements.

Commission of Acts or Omissions without Designation

Finding 3. NSIRA found that CSIS may not have been in compliance with subsection 20.1(11) of the CSIS Act when [#] employees committed acts or omissions that would otherwise constitute offences while not designated by the Minister.

Direction of Acts or Omissions without Authorization

Finding 4. NSIRA found that CSIS may not have been in compliance with subsections 20.1(12) and (15) of the CSIS Act when [#] employees directed acts or omissions that would otherwise constitute offences absent authorization from the Director or a designated senior employee.

Transparency and Accountability

Finding 5. NSIRA found that CSIS may not have been in compliance with subsection 20.1(23) of the CSIS Act in [#] operations when employees did not report in writing to the Director or a designated senior employee following the commission or direction of [#] acts or omissions that would otherwise constitute offences.

Finding 6. NSIRA found that CSIS may not have been in compliance with subsection 20.1(26)(c) of the CSIS Act when it did not notify NSIRA of all reports of commission or direction of acts or omissions that would otherwise constitute offences.

Finding 7. NSIRA found that the Minister of Public Safety may not have been in compliance with subsection 20.1(24) of the CSIS Act when they did not annually publish or

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

make available a report in respect of CSIS's use of the justification framework for 2019, 2020, 2021 or 2022.