UNCLASSIFIED

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

Review of Government of Canada Institutions' Disclosures of Information Under the *Security of Canada Information Disclosure Act* in 2023

NSIRA // Review 23-11

© His Majesty the King in Right of Canada, as represented
by the National Security and Intelligence Review Agency.
Ottawa, Ontario

Review of Government of Canada Institutions' Disclosures of Information Under the *Security of Canada Information Disclosure Act*

Title in French: Examen des communications d'information par les institutions fédérales au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*

2023
Annual
ISSN 2817-7525

Contact info@nsira-ossnr.gc.ca to obtain this document
in an alternate format for accessibility.

Table of Contents

Table of Contents ii

List of Acronyms iii

Glossary of Terms iv

Executive Summary v

1. Introduction 1

Authority 1
Scope of the Review 1
Methodology 1
Review Statements 1

2. Background 2

3. Findings, Analysis, and Recommendations 3

Volume and Trend Analysis 3
Record Keeping Requirements – Section 9 3
Contribution and Proportionality Tests – Subsection 5(1) 5
SCIDA's Exception for Advocacy, Protest, or Dissent 6
IRCC's New Approach to Proportionality Assessments 7
CSIS Request Letters 10
Reliability and Accuracy Statement – Subsection 5(2) 12
Information Sharing Agreement – Subsection 4(c) 14

4. Conclusion 15

Annex A. Sample of Disclosures 16

Annex B. Cases Relating to IRCC's Disclosure of Visa Information 17

Disclosure 1 (Economic Security Threat) 17
Disclosure 2 (Foreign Entity) 17
Disclosure 3 (Bulk Data) 18

Annex C. Overview of SCIDA Disclosures in Prior Years 19

Annex D. Findings and Recommendations 20

Record Keeping Requirements – Section 9 20
Contribution and Proportionality Tests – Subsection 5(1) 20
Reliability and Accuracy Statement – Subsection 5(2) 21
Information Sharing Agreement – Subsection 4(c) 21

List of Acronyms

CBSA	Canada Border Services Agency
CFIA	Canadian Food Inspection Agency
CNSC	Canadian Nuclear Safety Commission
CRA	Canada Revenue Agency
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DND/CAF	Department of National Defence/Canadian Armed Forces
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
GAC	Global Affairs Canada
GC	Government of Canada
ISA	Information-sharing arrangement
IRCC	Immigration, Refugees and Citizenship Canada
NSIRA	National Security and Intelligence Review Agency
PHAC	Public Health Agency of Canada
PS	Public Safety Canada
REP	Reasonable expectation of privacy
RCMP	Royal Canadian Mounted Police
SCIDA	*Security of Canada Information Disclosure Act*
TC	Transport Canada

Glossary of Terms

Contribution test The first part of the two-part threshold that must be met before an institution can make a disclosure under the SCIDA: it must be satisfied that the information will contribute to the exercise of the recipient institution's jurisdiction or responsibilities in respect of activities that undermine the security of Canada [paragraph 5(1)(a)].

Proportionality test The second part of the two-part threshold that must be met before an institution can make a disclosure under the SCIDA: it must be satisfied that the information will not affect any person's privacy interest more than reasonably necessary in the circumstances [paragraph 5(1)(b)].

Executive Summary

The objective of this review was to determine whether Government of Canada (GC) institutions complied with the *Security of Canada Information Disclosure Act* (SCIDA)'s requirements for disclosure and record keeping in 2023. The review assessed GC institutions' use of information-sharing arrangements, consistent with SCIDA's guiding principles. The review also documented the volume of SCIDA disclosures and highlighted patterns in the SCIDA's use across GC institutions and over time.

This is the fifth year that GC institutions have used the SCIDA and that NSIRA has reviewed their compliance with the act. Each year, NSIRA has made recommendations aimed at promoting compliance with the Act. Over the last five years, GC institutions have adjusted their practices and are increasingly demonstrating an improved understanding of their obligations. As a result, for the first time in SCIDA's history, NSIRA found full compliance with the SCIDA. This allowed NSIRA to focus its review on in-depth analysis of the SCIDA's contribution and proportionality tests.

For instance, some Immigration, Refugees and Citizenship Canada (IRCC) disclosures, albeit compliant with the SCIDA, presented a heightened risk of non-compliance with these two tests. One disclosure involving protest activity raised concerns regarding how IRCC arrived at the conclusion that the disclosure was related to activity that undermined the security of Canada, and thus complied with paragraph 5(1)(a) of the SCIDA. Three disclosures also raised concerns with regard to the amount of personal information that IRCC disclosed following its proportionality assessment, pursuant to paragraph 5(1)(b).

CSIS request letters, on which IRCC often relies to assess compliance with subsection 5(1), were at times unclear. This hindered IRCC's effort to satisfy itself that the disclosure was authorised under the SCIDA.

IRCC provided templated statements on accuracy and reliability that were not always relevant or specific to the circumstances of the disclosure. In one case, the Canada Border Services Agency (CBSA) made a verbal disclosure that did not include an explicit statement about accuracy and reliability at time of disclosure. In addition, CBSA's record of disclosure form contradicts the SCIDA by suggesting that the provision of information on accuracy and reliability is optional.

As encouraged by the SCIDA's guiding principles, and as recommended by NSIRA previously, IRCC and the Communication Security Establishment signed an information-sharing agreement.

NSIRA made seven recommendations to mitigate risks of non-compliance and enshrine best practices in future years.

1. Introduction

Authority

1. This review was conducted pursuant to subsections 8(1)(b) and 39(1) of the *National Security and Intelligence Review Agency Act* (NSIRA Act).
2. The review satisfies the NSIRA Act's section 39 requirement for NSIRA to submit a report to the Minister of Public Safety on disclosures made under the *Security of Canada Information Disclosure Act* (SCIDA, Act) during the previous calendar year.

Scope of the Review

3. The objective of this review was to determine whether Government of Canada (GC) institutions complied with the SCIDA's requirements for disclosure and record keeping. The review assessed GC institutions' use of information-sharing arrangements, consistent with SCIDA's guiding principles. The review also documented the volume of SCIDA disclosures and highlighted patterns in the SCIDA's use across GC institutions and over time.
4. The review included all GC institutions that disclosed or received information under the SCIDA in 2023: the Canada Border Services Agency (CBSA), Communications Security Establishment (CSE), Canadian Security Intelligence Service (CSIS), Global Affairs Canada (GAC), Immigration, Refugees and Citizenship Canada (IRCC), and Royal Canadian Mounted Police (RCMP). The review also included Public Safety Canada (PS), which provides SCIDA-related policy guidance and training across the GC.

Methodology

5. NSIRA assessed administrative compliance with the SCIDA's record keeping obligations in respect of all disclosures made in 2023.
6. NSIRA assessed substantive compliance with the SCIDA's disclosure requirements for a targeted sample of 27 disclosures, selected according to the parameters described in Annex A.

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.[1]

8. All reviewees met NSIRA's expectations for responsiveness during this review.

2. Background

9. The SCIDA provides an explicit, stand-alone authority to disclose information between GC institutions in order to protect Canada against activities that undermine its security. Its stated purpose is to encourage and facilitate such disclosures.

10. Section 9 of the SCIDA prescribes record-keeping obligations for all institutions who disclose or receive information under the Act. Subsection 9(3) requires that these records be provided to NSIRA within 30 days after the end of each calendar year.

11. Subsection 5(1) of the SCIDA authorizes GC institutions to disclose information – subject to any prohibitions or restrictions in other legislation or regulations – to designated recipient institutions if the disclosing institution is satisfied that (a) the information will contribute to the exercise of the recipient institution's jurisdiction or responsibilities in respect of activities that undermine the security of Canada (the "contribution test"); and (b) the information will not affect any person's privacy interest more than is reasonably necessary in the circumstances (the "proportionality test").

12. Subsection 5(2) requires disclosing institutions to, at the time of the disclosure, also provide information regarding the disclosure's accuracy and the reliability of the manner in which it was obtained.

13. When a GC institution receives information under the Act, subsection 5.1(1) requires that the institution destroy or return any unnecessary personal information as soon as feasible after receiving it.

14. The SCIDA's guiding principles reinforce the notion that effective and responsible disclosure of information protects Canada and Canadians. Of note, subsection 4(c) suggests that GC institutions enter into an information-sharing arrangement when they regularly disclose information to the same recipient.

---

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

3. Findings, Analysis, and Recommendations

Volume and Trend Analysis

15. In 2023, GC institutions made a total of 269 disclosures under the SCIDA (see Table 1).

Table 1: Number of SCIDA disclosures made in 2023 by disclosing and recipient institutions [all disclosures (proactive disclosures)]

		Designated Recipient Institutions																
		CBSA	CFIA	CNSC	CRA	CSE	CSIS	DND/CAF	Finance	FINTRAC	GAC	Health	IRCC	PHAC	PS	RCMP	TC	TOTAL (proactive)
Disclosing Institution	CBSA	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2 (2)	-	2 (2)
	GAC	-	-	-	-	1 (1)	10 (0)	-	-	-	-	-	-		-	4 (0)	-	15 (1)
	IRCC	-	-	-	-	58 (0)	194 (7)	-	-	-	-	-	-	-	-	-	-	252 (7)
	TOTAL (proactive)	-	-	-	-	59 (1)	204 (7)	-	-	-	-	-	-	-	-	6 (2)	-	269 (10)

16. The number of disclosures increased 55% since 2022, reversing the slight downward trend in the number of disclosures observed across prior years. This shift is largely due to a 246% increase in disclosures from IRCC to CSIS. CSIS attributes this increase to a policy shift that led them to use the SCIDA to request information that IRCC previously provided under the *Privacy Act.*

17. As in previous years, disclosing institutions made the vast majority of disclosures following a request. Only 4% of disclosures were sent proactively by the disclosing institution.

Record Keeping Requirements – Section 9

Finding 1. NSIRA found that every institution that disclosed or received information pursuant to SCIDA in 2023 complied with their record keeping obligations under section 9, but some records were inaccurate or imprecise.

18. Section 9 of the SCIDA prescribes record-keeping obligations for all disclosing institutions, as well as institutions who receive information pursuant to a disclosure.

These requirements include, among others, that records of the disclosure describe the information as well as indicate whether the information was destroyed or retained by the recipient. NSIRA's cross-reference of records provided by disclosing and recipient institutions revealed some inaccuracies that were clarified through discussion with the institutions following receipt of their records:

- Under paragraph 9(2)(a), CSE mislabelled the number of subjects that the disclosure pertained to in four (of 59) instances;
- Under paragraph 9(2)(e), CSIS records included contradictory information as to whether the information received has been destroyed or retained; and
- Under paragraph 9(1)(a), IRCC records included contradictory descriptions of the information disclosed.

19. NSIRA was unable to reconcile the information provided in relation to one case where the CBSA made a verbal disclosure to the RCMP. Based on the initial records provided by the RCMP and CBSA, NSIRA could not determine with certainty what personal information was shared, and when. In response to a recommendation from NSIRA's SCIDA review for 2022, the CBSA developed a record of disclosure form to serve as a record overview. In this instance, the form was incomplete and contradicted the copy of the disclosure that was also provided to NSIRA.

20. As it did last year, NSIRA underscores the importance of administrative precision in preparing records, and notes that a record overview – when correctly prepared – supports compliance with SCIDA record keeping requirements.

21. NSIRA identified several instances in which the disclosing institution did not provide an explicit statement, under paragraph 9(1)(e), regarding the information that was relied on to satisfy the disclosing institution of the proportionality test.[2] Three of these disclosures were included in NSIRA's targeted sample for assessing the contribution and proportionality tests.

[2] This number reflects an improvement over NSIRA's SCIDA review for 2022, which found that more than half of the descriptions provided by CBSA and IRCC under paragraph 9(1)(e) of the SCIDA did not explicitly address their satisfaction that the disclosure was authorized under paragraph 5(1)(b), the proportionality test.

Contribution and Proportionality Tests – Subsection 5(1)

Finding 2. NSIRA found, within the sample of disclosures reviewed, that disclosing institutions demonstrated they had satisfied themselves under the contribution and proportionality tests in compliance with subsection 5(1) of the SCIDA.

22. To assess compliance with subsection 5(1), NSIRA first considered the explicit statements prepared by disclosing institutions under paragraph 9(1)(e), describing the information that was relied on to satisfy themselves that the disclosure was authorized under the Act. When an explicit statement was provided, NSIRA analysed and corroborated these statements by reviewing all other documents provided by GC institutions related to a given disclosure. Additional documents provided did not raise any concern with paragraphs 5(1)(a) and 5(1)(b) compliance.

23. For all 27 disclosures included in the sample, the disclosing institution provided an explicit statement that demonstrated that they had satisfied themselves that the disclosure would contribute to the recipient's jurisdiction or its responsibilities.

24. For 24 of the 27 disclosures, the disclosing institution provided an explicit statement that demonstrated they had satisfied themselves that no one's privacy would be affected more than reasonably necessary in the circumstances. In the remaining three disclosures, despite having no explicit statement, other documents provided by the disclosing institutions nevertheless demonstrated that they had satisfied themselves of the proportionality test.

25. While NSIRA found that institutions were generally compliant with paragraphs 5(1)(a) and 5(1)(b), IRCC's contribution and proportionality assessments demonstrated some deficiencies. These deficiencies form the basis of findings 3 and 4.

Recommendation 1. NSIRA recommends that disclosing institutions explicitly address the requirements of both paragraphs 5(1)(a) and 5(1)(b) in the records that they prepare under paragraph 9(1)(e) of the SCIDA.

SCIDA's Exception for Advocacy, Protest, or Dissent

Finding 3. NSIRA found that IRCC did not, in one instance, independently consider whether its disclosure related to activities that fell under the SCIDA exception for advocacy, protest, or dissent. Instead, IRCC satisfied itself of the SCIDA's contribution test based on assumptions about how CSIS assessed activities that undermine the security of Canada.

26. The contribution test under paragraph 5(1)(a) requires the disclosing institution to assess whether the disclosure relates to activities that undermine the security of Canada. These activities are defined by the Act and include, for example, espionage, covert foreign-influenced activities, terrorism, and significant or widespread interference with critical infrastructure. In its definition of activities that undermine the security of Canada, subsection 2(2) of the SCIDA includes an exception for advocacy, protest, dissent, or artistic expression. These, in and of themselves, do not constitute activities that undermine the security of Canada. The legislated exception helps to distinguish between legitimate forms of political dissent and national security threats.

27. In one instance, CSIS requested detailed information from IRCC related to an individual. The request sought current and past passport applications and these contain a great deal of personal information[3].CSIS justified its request with an excerpt from a news article which cited a quote uttered publicly by the individual during a protest.

28. IRCC did not request any additional rationale from CSIS. It disclosed the individual's passport application, including some associate's information, along with the individual's passport number, place of issue, and dates of issue and expiry.

29. In response to a query from NSIRA regarding on what basis it satisfied itself of the contribution test, IRCC explained that it "relies on the partner to accurately describe that the individual is tied to an activity that may undermine the security of Canada." The IRCC official who authorized the disclosure further explained that IRCC assumed that CSIS had not relied solely on the individual's statements quoted in the news article given the limits of CSIS's authority to investigate lawful advocacy, protest or dissent under the CSIS Act.

[3] IRCC applications request information such as place of birth, marital status, photograph, employment history, current and past home addresses, telephone and emails addresses, information on associates (reference, emergency contact, guarantor), and passport information.

30. The CSIS Act includes an exemption preventing CSIS from investigating lawful advocacy, protest or dissent, without the presence of threat related activities itemised in the CSIS Act. However, the SCIDA's use of "activity that undermines the security of Canada" is a purposeful departure from the CSIS Act's "threat to the security of Canada". The distinction reflects legislative intent that the disclosing institution perform its own, fit-for-purpose assessment.

31. Subsection 5(1) of the SCIDA explicitly places the onus on the disclosing entity to assure itself that the disclosure is authorized. The process by which an institution satisfies itself should be grounded in an independent and factual assessment. In that context, a mere acquiesce of a request would not be sufficient, nor would a *de facto* reliance on the recipient respecting their enabling legislation. The threshold of satisfaction imports an objective standard that must be based on facts.

32. PS guidance notes that although the threshold imposed by subsection 5(1) does not hold institutions to perfection, they must make all reasonable efforts to satisfy themselves that the information will contribute to the recipient's national security mandate. When encountering activities occurring in the context of political dissent or a protest, NSIRA expects institutions with a national security mandate to exercise caution when requesting information relating to an activity protected under the *Canadian Charter of Rights and Freedoms* (Charter) to further an investigation. At the same time, in this case, IRCC should have obtained more information prior to disclosure, to substantiate what activities were undermining the security of Canada to ensure the exception did not apply.

Recommendation 2. NSIRA recommends that IRCC amend their SCIDA policy to underscore that IRCC must independently assess whether the disclosure is authorized. This assessment should consider whether the activity amounts to one of the exceptions to the SCIDA's definition of activities that undermine the security of Canada.

IRCC's New Approach to Proportionality Assessments

Finding 4. NSIRA found that, throughout the course of 2023, IRCC improved the rigour of its proportionality assessments regarding disclosure of passport information. However, NSIRA identified three instances where IRCC disclosed visa information without applying the same rigorous approach, which risked disclosing more personal information than reasonably necessary in the circumstances.

33. In summer 2023, IRCC adopted a "higher" standard to satisfy itself that no person's privacy interest would be affected more than reasonably necessary when disclosing passport information to CSIS. According to IRCC, this shift was prompted by a previous NSIRA recommendation that IRCC be explicit in their records that the proportionality test was met. Not only did IRCC adjust their record keeping practices, but they also turned their attention to the substantive issue at hand. Indeed, IRCC closely examined the privacy impact their disclosures may have when responding to CSIS requests.

34. As a result, when dealing with the absence of additional rationale from CSIS, IRCC became more conservative in the disclosure of information. For example, IRCC began redacting associate's information in passport applications, limiting the provision of historical applications, and refraining from disclosing applications of minors. They adopted an iterative approach[4] to disclosing passport information, which cultivated a more appropriate weighting of individuals' privacy interests vis-à-vis the recipient's investigative needs.

35. IRCC's new approach to assessing the proportionality of passport information disclosures was not well-received by CSIS, who characterize their receipt of redacted passport applications as a "massive" hindrance to section 12 investigations.[5] In internal correspondence, a CSIS analyst noted that they would prefer that "IRCC not filter down the info and let them [CSIS] make the assessment based on the knowledge of [national security] threats".

36. Still, the discretionary nature of SCIDA disclosures make it such that IRCC may choose what information to disclose, if any. IRCC's SCIDA Standard Operating Procedure states that requests for disclosure must provide sufficient information to justify the release of associate's information. Under the SCIDA, it is entirely within

[4] An iterative approach is a method of decision-making that involves repeating a series of steps in a cycle until the desired outcome is achieved. It is characterized by continuous improvement and adaptation based on feedback and results.

[5] Subsection 12(1) of the CSIS Act, usually referred to as section 12 authority, is one of the main provisions in the CSIS Act. This is the provision that allows CSIS to collect and retain information and intelligence on activities constituting threats to Canada within the meaning of section 2 of the CSIS Act, to the extent that it is strictly necessary. A significant portion of CSIS activities rely on this authority for their lawfulness. CSIS interprets the section 12 collection and retention thresholds broadly: "[a]s long as, the Service thinks the information can help get to information about the threat(s), the Service can collect and retain". This interpretation collides with the SCIDA requirement that each piece of information disclosed must not affect an individual's privacy interest more than reasonably necessary.

IRCC's purview to seek and obtain such justification prior to disclosing information.[6]

37. IRCC's increased attention to privacy interests in the context of passport application disclosures was not imparted to disclosures of information collected from visa applications. It is important to note that this distinction is not a factor that should be considered when assessing proportionality. Under the SCIDA, the privacy interests of citizens and non-citizens must be similarly assessed, and only treated differently in a visa application if no reasonable expectation of privacy is assessed.[7]

38. Annex B presents the details of three disclosures in relation to which IRCC disclosed visa information to CSIS, concerning over 20 individuals, without having first established facts relevant to the conduct of an informed proportionality assessment. In these cases, either the identities of the subject of the request were unknown[8] or the link between the subject of the disclosure and the threat had yet to be established. NSIRA would have expected IRCC to follow a more iterative approach to disclosing this information, consistent with its approach to passport disclosures in the later part of 2023. Such an iterative approach would have entailed disclosing only basic information until a greater connection to the activity that undermined the security of Canada could be established or the identity of the individual could be confirmed.

39. Additionally, the cases presented in Annex B are not fully consistent with IRCC policy, which underscores that "disclosing [...] more personal information than is necessary could constitute a breach of a person's reasonable expectation of privacy, a right protected by the Canadian Charter of Rights and Freedoms". This is an important consideration since the proportionality of a given disclosure may be a factor in determining its Charter reasonableness.

---

[6] IRCC and CSIS signed an information sharing agreement to govern their information exchanges under the SCIDA in May 2024. It is apparent to NSIRA, however, that there remains important disagreement regarding how IRCC ought to conduct the proportionality test and what information should be released to CSIS following a request.

[7] For the purpose of SCIDA, the disclosing institution must satisfy itself that the disclosure will not affect any person's privacy interest (territorial privacy, informational privacy; and personal privacy) more than is reasonably necessary in the circumstances. The legal threshold for what is reasonably necessary in the circumstances will be very similar to the concept of a reasonable expectation of privacy (REP) in Charter jurisprudence. REP is the same for citizens and non-citizens when they are within the jurisdiction of Canada. However, the Charter has only limited applicability extraterritorially and while such limits may include Canadian citizens abroad, they do not include foreign nationals outside of Canada without at nexus to Canada. While a person in an immigration or travel context has a diminished REP, it does not create a Charter-free zone. Therefore, a person's privacy interest assessment should follow a similar analytical framework under SCIDA regardless of their citizenship status.

[8] In most cases, CSIS requests include a name and a date of birth that IRCC uses to query. In rare cases, CSIS does not provide IRCC with names or birth date, but with search parameters that would help to identify the individual.

40. Under the SCIDA regime, and as explained in PS guidance, the proportionality test is conducted to help determine the scope of what can be disclosed, and not necessarily whether the disclosure should occur. Thus, it would have been warranted for IRCC to assess how the sharing of each piece of information would impact the privacy of the individuals in question.

Recommendation 3. NSIRA recommends that IRCC apply an iterative approach to its proportionality assessments, with a view to disclosing only the minimum information reasonably necessary in the circumstances to enable the recipient institution to further their investigation.

CSIS Request Letters

Finding 5. NSIRA found that CSIS requests to IRCC used inconsistent terminology and were often unclear about the relationship between the subject of the request and its investigation. At times, this lack of clear communication hindered IRCC's efforts to satisfy itself that the disclosure was authorised under the SCIDA.

41. 96% of IRCC disclosures to CSIS were in response to a request. IRCC used the information in CSIS's request letters to assure itself that a disclosure met both the contribution and the proportionality tests. While IRCC is always at liberty to request more information from CSIS to satisfy itself that the disclosure is authorized, in the majority of disclosures requested by CSIS, IRCC based its assessments solely on the information provided by CSIS in the request letter.

42. NSIRA reviewed all request letters sent by CSIS to IRCC. CSIS used a wide variety of terms to describe the nature of its interest in the subject of a request, such as:

    - The subject came to the attention of the Service
    - The subject is of interest for possible involvement in
    - The subject is of interest in connection with
    - The subject is believed to be an associate of a target
    - The subject is related to the threat
    - The individual is the subject of a Service investigation
    - The subject is part of a Service investigation
    - The subject is very closely associated to a CSIS subject of investigation

    In most cases, CSIS did not define these terms or provide any more information on why the subject was of interest.

43. Furthermore, CSIS used the same (or similar) words when referring to different levels of interest. For example, “associated with” and “part of a Service Investigation” were used in requests for individuals with no known involvement in threat related activities and for individuals who CSIS has reason to suspect are involved in threat activities. In another instance, CSIS’s request letter stated that the subjects were related to the threat, but the connection between the threat and the individuals had not been established.

44. As a result of these inconsistencies and lack of clarity, IRCC could not understand key nuances relevant to its proportionality assessments. This issue is compounded by the fact the CSIS tended to request “any and all information” associated with the subject(s) of a request.

45. The relationship between the information requested and an investigation is an important factor considered by IRCC when assessing proportionality. Indeed, IRCC’s new approach to assessing proportionality takes into consideration the fact that information on associates contained in passport applications may not be material to the investigation. As a result, IRCC has often opted to redact some associate’s information, unless CSIS provided some indication that they are, or could be, implicated in the threat activity. In one of the several instances where CSIS stated that the subject of the request was “very closely associated to a CSIS subject of investigation”, IRCC requested an explanation to clearly link the subject of the request to the investigation. When CSIS did not provide it, IRCC opted to cancel the disclosure as it was not satisfied that the disclosure would meet the proportionality test.

46. It is essential that CSIS convey information in a clear and consistent manner given that IRCC takes this information into account in conducting its proportionality assessments. This is especially true when IRCC is disclosing associate’s information. When requesting information under the SCIDA, recipient institutions should, as a matter of course, facilitate disclosing institutions’ compliance with SCIDA thresholds by using clear and consistent terminology.

47. In late 2023, CSIS began centralizing its process for requesting IRCC SCIDA disclosures and developed a standard request form, which should help with consistency. As no requests were made in 2023 using these standard forms, NSIRA could not assess the effect of these changes in practice.

Recommendation 4. NSIRA recommends that CSIS use consistent terminology, and be clear about the nature of the link that has been established between the subject of a request and its investigation, to assist IRCC in satisfying itself of the proportionality test.

Reliability and Accuracy Statement – Subsection 5(2)

Finding 6. NSIRA found that disclosing institutions provided information regarding the accuracy of the information and reliability of the manner in which it was obtained in relation to all disclosures. However, CBSA made one verbal disclosure that did not include an explicit statement on accuracy and reliability.

48. Under the SCIDA, departments are required to provide information on the accuracy and the reliability of the manner in which the information being disclosed was obtained. They must do so at the time of the disclosure.

49. All written disclosures made in 2023 contained a statement on accuracy and reliability. However, CBSA made one proactive verbal disclosure of a tip to the RCMP, previously described in paragraph 19, in which it did not provide an explicit statement regarding accuracy and reliability at the time of disclosure.

50. Although the same information was shared again in writing two weeks later, an explicit, written statement on accuracy and reliability was only shared with the RCMP nearly two months later, when the CBSA disclosed additional information about the subject.

51. Subsection 5(2) states that “information” regarding accuracy and reliability “must” be provided at time of disclosure. NSIRA assesses in this case that, by its very nature, relaying that the information disclosed was derived from a tip conveyed information regarding accuracy and reliability to the RCMP. That said, an explicit, written statement is considered best practice. While verbal disclosures are not prohibited by the SCIDA, PS guidance notes that “[i]nformal communication cannot be used in lieu of the formal disclosure process or to replace the formal record-keeping obligations.”

Recommendation 5. NSIRA recommends that institutions avoid making verbal disclosures whenever possible. When they must occur, verbal disclosures should explicitly convey the requisite information on accuracy and reliability.

Finding 7. NSIRA found that CBSA’s record of disclosure form contradicts the SCIDA by allowing officials to opt out of providing information regarding accuracy and reliability.

52. Although CBSA policy correctly reflects the mandatory nature of providing information on accuracy and reliability, its new record of disclosure form does not. The form includes a yes/no checkbox to indicate whether a statement confirming the accuracy and reliability was provided to the recipient institution. If the CBSA official selects “no”, they are prompted to explain why they elected to not provide a statement. This implies that it is discretionary and leaves the opportunity for CBSA to opt out of the requirement.

53. Further, the form does not specify that the statement must be provided at the time of disclosure, as the SCIDA specifically demands.

Recommendation 6. NSIRA recommends that CBSA harmonize its record of disclosure form with the SCIDA to convey the mandatory nature of providing information on accuracy and reliability at the time of the disclosure.

Finding 8. NSIRA found that IRCC used templated language to describe the disclosure’s accuracy and reliability that was not always relevant or specific to the circumstances of the disclosure.

54. All IRCC disclosures made in 2023 included the same accuracy and reliability statement:

> *The information in this disclosure was provided by the Subject as part of their various applications to IRCC. The Subject declared that the information they provided as part of their applications was truthful, complete and correct. The information in this disclosure is accurate and reliable in so far as the Subject was truthful in their submissions to our Department. IRCC holds no information that would call into question the accuracy and reliability of the information provided by the Subject*.

55. There are several cases where this statement provided by IRCC did not reflect the specific circumstances of the disclosure. For example, the statement above was included in a disclosure where no immigration or passport records were found and the only information disclosed was the lack of records. The same statement was used in disclosures of child general passport applications, which are actually completed by parents or legal guardians rather than by the subject themselves. When solely disclosing citizenship status to CSE, IRCC still included the same statement, despite the information disclosed not being provided by the subject as part of their application. In one case, the IRCC used the same statement in the

disclosure but nevertheless contradicted itself by also stating that there was some reason to believe the information might not be accurate.

56. All of these cases point to a tendency of copying the accuracy and reliability information without giving sufficient attention to the relevance of the statement.

57. When instructing on the accuracy and reliability statement, the PS SCIDA guide suggests that "formulaic (templated) language should be avoided, unless the nature and source of information disclosed is derived from a routine process." IRCC produces a large number of disclosures every year. While some language can be recycled, it is necessary that the statement remain an accurate representation of each disclosure. NSIRA has previously recommended that statements be clear and specific to the circumstances of the disclosure.

Recommendation 7. NSIRA recommends that IRCC tailor its statements on accuracy and reliability as to ensure that each disclosure's statement is specific to the circumstances of the case.

Information Sharing Agreement – Subsection 4(c)

Finding 9. NSIRA found that disclosures between IRCC and CSE that occurred following the enactment of their new information sharing agreement were compliant with both the SCIDA and their information sharing agreement.

58. In past SCIDA reviews, NSIRA noted that some departments regularly use the SCIDA in a manner that warrants information sharing arrangements (ISA), as encouraged by subsection 4(c) of SCIDA. In 2022, NSIRA recommended that IRCC and CSE develop an ISA to govern their SCIDA disclosures.

59. In August 2023, IRCC and CSE signed an ISA. As a whole, the new ISA between IRCC and CSE supports compliance with SCIDA, with all key legislated requirements from SCIDA being included in the ISA. The agreement also adheres to the guidance on preparing ISAs recently developed by PS.

60. Of the 24 disclosures made after the ISA implementation, all were deemed compliant with the new agreement. NSIRA looked at each disclosure made under the ISA and assessed them against a majority of the requirements outlined in the agreement.

4. Conclusion

61. This is the fifth year that GC institutions have used the SCIDA and that NSIRA has reviewed their compliance with the act. Each year, NSIRA has made recommendations aimed at promoting compliance with the Act. Over the last five years, GC institutions have adjusted their practices and are increasingly demonstrating an improved understanding of their obligations. As a result, for the first time in SCIDA's history, NSIRA found full compliance with the SCIDA.

62. This review assessed GC institutions' compliance with requirements for record keeping in respect of all 269 disclosures that were made and received in 2023. It assessed their compliance with requirements for disclosure in relation to a targeted sample of 27 disclosures. All were compliant with SCIDA requirements, but NSIRA found that IRCC's contribution and proportionality assessments demonstrated some deficiencies. An increased understanding of the activities that undermine the security of Canada would support a more thorough proportionality assessment and greater utility of the disclosed information.

63. NSIRA made recommendations aimed at promoting compliance with SCIDA, particularly with regard to how departments determine whether the contribution and proportionality tests have been met.

Annex A. Sample of Disclosures

Disclosures were selected for the sample based on the content of records provided to NSIRA under subsection 9(3), according to the following parameters:

- At least two disclosures per discloser-recipient pair, if available;
- At least one proactive disclosure per discloser, if available;
- At least one requested disclosure per recipient, if available;
- All disclosures identified by recipient institutions as including personal information that was destroyed or returned under the SCIDA, subsection 5.1(1);
- All disclosures for which there is a high-level discrepancy in the discloser and recipient records;
- All disclosures made by an institution that is not listed in Schedule 3 of the SCIDA;
- All disclosures received by institutions added to Schedule 3 in the preceding year; and
- All disclosures that, based on the review team's preliminary assessment, present a heightened risk of non-compliance under section 5.

Annex B. Cases Relating to IRCC's Disclosure of Visa Information

Disclosure 1 (Economic Security Threat)

64. IRCC proactively disclosed to CSIS the visa applications of several individuals who received a work permit in various research fields linked to economic security threat. These applications included personal information such as employment history, travel history, contact information, photos, passport information, and associate's information. This was part of IRCC's effort to proactively identify and share with CSIS information about individuals that may engage in activities that pose a threat to Canada's economic prosperity.

65. While the national security concern posed by these types of economic security threats is well documented, the role that these individuals played in that space was unknown. IRCC selected the individuals in question based on one threat related criteria, but the other criteria used to narrow the pool individuals from several hundreds to a few individuals were unrelated to the threat the individuals posed. Indeed, IRCC chose these additional arbitrary criteria mainly for practical reasons.

66. For greater clarity, there was no information indicating that any of the several individuals in question were involved in activities that undermine the security of Canada. Most of these applications were not initially referred to CSIS for security screening by IRCC, meaning that the visa officer was fully satisfied that the applicants posed no threat. In one case, the application was sent for security screening but CSIS returned a favorable recommendation and the individual was granted a visa.

67. The proactive sharing of complete visa application packages with CSIS risked affecting these individuals' privacy more than was reasonably necessary in the circumstances.

Disclosure 2 (Foreign Entity)

68. CSIS requested passport information about any individuals with a valid visa currently working for a specific foreign entity. IRCC did not have any passport applications for the individuals that matched the search criteria, but nevertheless disclosed entire visa applications for some individuals. IRCC also provided information about individuals who had previously worked at the foreign entity, and individuals who did not have a valid visa. This misalignment between what was requested and what was disclosed does not reflect a proper tailoring of information to meet SCIDA's contribution and proportionality tests.

69. None of these individuals had been linked to a specific activity that undermined the security of Canada, either at the time of the request nor following the disclosure. CSIS and IRCC's inability to characterize the nature of the individuals' relationship to threat activities created a risk that IRCC's disclosure may have affected their privacy more than was reasonably necessary in the circumstances.

Disclosure 3 (Bulk Data)

70. CSIS sent a letter to IRCC requesting the disclosure of information within immigration applications on individuals including a spreadsheet with certain identifying personal information (called "selectors"). While large data-set requests and disclosures are not prohibited by the SCIDA, the requirements imposed by the contribution and proportionality tests must be applied to every discrete piece of information disclosed. As such, this type of information would need to be responsibly assessed prior to disclosure.

71. While the CSIS request letter provides extensive rationale as to why the threat actor named in the request letter poses a threat to national security, the IRCC officials that authorized the disclosure did not have contemporaneous information on how these selectors, and, by extension the individuals linked to these selectors, are linked to the threat actor.

72. Nevertheless, IRCC disclosed significant personal details pertaining to several individuals. For example, the disclosure included a foreign state visa refusal, information about military service, a personal picture, and other documents that would have been provided as part of a visa application.

73. This disclosure included more information than what CSIS requested. Given that the identity of the individuals are unconfirmed, as CSIS's request clearly stated that the purpose of this request was for identification, this suggests that IRCC risked disclosing more than the least amount of personal information necessary for CSIS to further its investigation.

74. While the legislative burden to ensure that the disclosure is authorized under SCIDA falls on the disclosing entity, in this case IRCC, it may be very complex for a disclosing entity to discharge its obligation under paragraphs 5(1)(a) and 5(1)(b) with these types of large data-sets requests, particularly when the requester provides very little rationale linking each selector or individual to the activity that undermines the security of Canada.

Annex C. Overview of SCIDA Disclosures in Prior Years

		Designated Recipient Institutions under the SCIDA, Schedule 3																
	Disclosing Institution[9]	CBSA	CFIA	CNSC	CRA	CSE	CSIS	DND/CAF	Finance	FINTRAC	GAC	Health	IRCC	PHAC	PS	RCMP	TC	**TOTAL**
2022	CBSA															4		**4**
	GAC						39	2								12		**53**
	IRCC					59	56											**115**
	RCMP												1					**1**
	TOTAL					59	95	2					1			16		**173**
2021	DND/CAF	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	**2**
	GAC	-	-	-	-	-	41	-	-	-	-	-	1	-	-	2	-	**44**
	IRCC	-	-	-	-	68	79	-	-	-	2	-	-	-	-	-	-	**149**
	TOTAL	**-**	**-**	**-**	**-**	**68**	**122**	**-**	**-**	**-**	**2**	**-**	**1**	**-**	**-**	**2**	**-**	**195**
2020	CBSA	-	-	-	-	-	1	-	-	-	-	-	-	-	-	3	-	**4**
	GAC	-	-	-	-	1	25	-	-	-	-	-	1	-	-	13	-	**40**
	IRCC	-	-	-	-	60	61	-	-	-	-	-	-	-	-	37	1	**159**
	RCMP	-	-	-	-	-	-	1	-	-	3	-	5	-	-	-	-	**9**
	TC	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	**2**
	Other[10]	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	**1**
	TOTAL	**-**	**-**	**-**	**-**	**61**	**88**	**1**	**-**	**-**	**3**	**-**	**6**	**-**	**-**	**55**	**1**	**215**
2019[11]	CBSA	-	-	-	-	-	1	-	-	-	-	-	-	-	-	2	-	**3**
	GAC	-	-	-	-	-	23	-	-	-	-	-	3	-	1	15	-	**42**
	IRCC	-	-	-	-	5	17	1	-	-	-	-	-	-	-	36	-	**59**
	RCMP	-	-	-	4	-	-	-	-	1	3	-	1	-	-	-	-	**9**
	TC	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	**1**
	TOTAL	**-**	**-**	**-**	**4**	**5**	**41**	**1**	**-**	**1**	**3**	**-**	**4**	**-**	**1**	**54**	**-**	**114**

[9] Nearly 200 institutions are authorized to make disclosures under the SCIDA. This table identifies only those that made disclosures in the associated year.

[10] Institution not listed in Schedule 3 of the Act [redacted in NSIRA's SCIDA review for 2020 (Review No. 21-13)].

[11] The SCIDA entered into force on June 21, 2019. The figures in this table accordingly reflect the period of June 21 – December 31, 2019.

Annex D. Findings and Recommendations

Record Keeping Requirements – Section 9

Finding 1. NSIRA found that every institution that disclosed or received information pursuant to SCIDA in 2023 complied with their record keeping obligations under section 9, but some records were inaccurate or imprecise.

Contribution and Proportionality Tests – Subsection 5(1)

Finding 2. NSIRA found, within the sample of disclosures reviewed, that disclosing institutions demonstrated they had satisfied themselves under the contribution and proportionality tests in compliance with subsection 5(1) of the SCIDA.

Recommendation 1. NSIRA recommends that disclosing institutions explicitly address the requirements of both paragraphs 5(1)(a) and 5(1)(b) in the records that they prepare under paragraph 9(1)(e) of the SCIDA.

Finding 3. NSIRA found that IRCC did not, in one instance, independently consider whether its disclosure related to activities that fell under the SCIDA exception for advocacy, protest, or dissent. Instead, IRCC satisfied itself of the SCIDA's contribution test based on assumptions about how CSIS assessed activities that undermine the security of Canada.

Recommendation 2. NSIRA recommends that IRCC amend their SCIDA policy to underscore that IRCC must independently assess whether the disclosure is authorized. This assessment should consider whether the activity amounts to one of the exceptions to the SCIDA's definition of activities that undermine the security of Canada.

Finding 4. NSIRA found that, throughout the course of 2023, IRCC improved the rigour of its proportionality assessments regarding disclosure of passport information. However, NSIRA identified three instances where IRCC disclosed visa information without applying the same rigorous approach, which risked disclosing more personal information than reasonably necessary in the circumstances.

Recommendation 3. NSIRA recommends that IRCC apply an iterative approach to its proportionality assessments, with a view to disclosing only the minimum information reasonably necessary in the circumstances to enable the recipient institution to further their investigation.

Finding 5. NSIRA found that CSIS requests to IRCC used inconsistent terminology and were often unclear about the relationship between the subject of the request and its investigation. At times, this lack of clear communication hindered IRCC's efforts to satisfy itself that the disclosure was authorised under the SCIDA.

Recommendation 4. NSIRA recommends that CSIS use consistent terminology, and be clear about the nature of the link that has been established between the subject of a request and its investigation, to assist IRCC in satisfying itself of the proportionality test.

Reliability and Accuracy Statement – Subsection 5(2)

Finding 6. NSIRA found that disclosing institutions provided information regarding the accuracy of the information and reliability of the manner in which it was obtained in relation to all disclosures. However, CBSA made one verbal disclosure that did not include an explicit statement on accuracy and reliability.

Recommendation 5. NSIRA recommends that institutions avoid making verbal disclosures whenever possible. When they must occur, verbal disclosures should explicitly convey the requisite information on accuracy and reliability.

Finding 7. NSIRA found that CBSA's record of disclosure form contradicts the SCIDA by allowing officials to opt out of providing information regarding accuracy and reliability.

Recommendation 6. NSIRA recommends that CBSA harmonize its record of disclosure form with the SCIDA, to convey the mandatory nature of providing information on accuracy and reliability at the time of the disclosure.

Finding 8. NSIRA found that IRCC used templated language to describe the disclosure's accuracy and reliability that was not always relevant or specific to the circumstances of the disclosure.

Recommendation 7. NSIRA recommends that IRCC tailor its statements on accuracy and reliability as to ensure that each disclosure's statement is specific to the circumstances of the case.

Information Sharing Agreement – Subsection 4(c)

Finding 9. NSIRA found that disclosures between IRCC and CSE that occurred following the enactment of their new information sharing agreement were compliant with both the SCIDA and their information sharing agreement.