



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 2024

NSIRA // Review 25-01

© His Majesty the King in Right of Canada, as represented
by the National Security and Intelligence Review Agency, 2025.

ISSN: 2817-7525

Catalogue No. PS106-10E-PDF

Table of Contents

- [Executive Summary](#)..... ii**
- [List of Abbreviations](#)..... iii**
- [Glossary of Terms](#)..... iv**
- [I. Introduction](#) 1**
 - [Authority](#) 1
 - [Scope](#)..... 1
 - [Methodology](#)..... 1
 - [Review Statements](#) 2
- [II. Background](#) 2**
- [III. Findings, Analysis, and Recommendations](#) 3**
 - [Volume and Trend Analysis](#) 3
 - [Record Keeping Requirements – Section 9](#) 4
 - [Information Sharing Agreements – Subsection 4\(c\)](#) 5
 - [Disclosure of Information Requirements – Section 5](#)..... 6
 - [Disclosure 1](#) 7
 - [Disclosure 2](#)..... 7
 - [Disclosure 3](#)..... 8
 - [Contribution and Proportionality Tests – Section 5\(1\)](#) 9
 - [Requirement to Destroy or Return – Subsection 5.1\(1\)](#) 11
- [IV. Conclusion](#)..... 12**
- [Annex A. Historical SCIDA Disclosures](#)..... 13**
- [Annex B. Findings and Recommendations](#) 14**

Executive Summary

This review assessed Government of Canada (GC) institutions' compliance with the disclosure and record-keeping requirements of the Security of Canada Information Disclosure Act (SCIDA) throughout 2024. The review also captured the volume of SCIDA disclosures and identified trends in its application across GC institutions over time.

NSIRA found that 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 the Royal Canadian Mounted Police (RCMP) generally complied with their record-keeping obligations under the SCIDA.

Due to the substantial increase of nearly 300% in disclosures from IRCC to CSIS in 2024, NSIRA focused its review primarily on these two institutions.

During the review period, IRCC and CSIS implemented a tiered request and disclosure process which reduced the amount of third-party information disclosed by IRCC, contributing to enhanced compliance with the SCIDA. However, NSIRA found instances when the information provided to IRCC by CSIS was limited and hampered IRCC's ability to fulfill its obligations as a disclosing institution to satisfy itself that the information disclosed is in respect of an activity that undermines the security of Canada.

In addition, NSIRA found that IRCC lacked a formal policy governing the disclosure of information about minors.

NSIRA found that CSE, in three of its requests for information under the SCIDA, provided IRCC with more information than was relevant to its disclosures.

NSIRA made four recommendations designed to ensure that institutions minimize the privacy impact to individuals in their requests and disclosures under the SCIDA.

With regard to the SCIDA's requirement in subsection 5.1(1) that recipient institutions destroy or return unnecessary personal information, NSIRA found that CSIS may not have complied in its retention of one disclosure containing erroneous personal information.

List of Abbreviations

CBSA	Canada Border Services Agency
CFIA	Canada 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
IRCC	Immigration, Refugees and Citizenship Canada
ISA	Information Sharing Agreement
NSIRA	National Security and Intelligence Review Agency
PHAC	Public Health Agency of Canada
PS	Public Safety Canada
RCMP	Royal Canadian Mounted Police
SCIDA	<i>Security of Canada Information Disclosure Act</i>
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 institutions' 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)].

I. Introduction

Authority

1. This review was conducted under the authority of paragraphs 8(1)(a), 8(1)(b), and subsection 39(1) of the *National Security and Intelligence Review Agency Act* (“NSIRA Act”).¹
2. In accordance with section 39 of the NSIRA Act, this review fulfills NSIRA’s requirement to submit an annual report to the Minister of Public Safety regarding disclosures made under the *Security of Canada Information Disclosure Act* (SCIDA, or the Act) in the preceding calendar year.

Scope

3. The objective of this review was to assess Government of Canada (GC) institutions’ compliance with the SCIDA’s disclosure and record-keeping requirements in 2024. The review also tracked the volume of SCIDA disclosures, analyzed usage patterns across institutions and over time, and examined how GC institutions employed information-sharing agreements.
4. The review’s assessment of compliance was limited to GC institutions that disclosed or received information under the SCIDA in 2024: 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 the Royal Canadian Mounted Police (RCMP).

Methodology

5. The review was primarily based on records provided to NSIRA by disclosing and recipient institutions under subsection 9(3) of the SCIDA. It was supplemented by an examination of the institutions’ SCIDA policies and procedures, as well as their responses to related information requests.
6. NSIRA assessed administrative and substantive compliance with the SCIDA’s record-keeping requirements for all disclosures made by CBSA, CSE, GAC, and the RCMP.

¹ SC 2019, c 13 [NSIRA Act].

With respect to disclosures from IRCC to CSIS, NSIRA reviewed a random representative sample of 250 disclosures.

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. CBSA, CSE, CSIS, GAC, and the RCMP met NSIRA's expectations for responsiveness during this review. IRCC only partially met NSIRA's expectations for responsiveness, given extended delays in IRCC's responses to requests for information.

II. 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”).

² NSIRA's “Expectations for Responsiveness in Reviews” are online at <https://nsira-ossnr.gc.ca>.

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.

III. Findings, Analysis, and Recommendations

Volume and Trend Analysis

Finding 1. NSIRA found that IRCC's disclosures to CSIS under the SCIDA increased significantly in 2024.

15. In 2024, GC institutions made a total of 900 disclosures under the SCIDA (see Table 1). The number of disclosures increased 235% overall since 2023.

Table 1: Number of SCIDA disclosures made in 2024, by disclosing and recipient institution [all disclosures (proactive disclosures)]

		Designated Recipient Institutions															TOTAL (proactive)	
		CBSA	CFIA	CNSC	CRA	CSE	CSIS	DND/CAF	Finance	FINTRAC	GAC	Health	IRCC	PHAC	PS	RCMP		TC
Disclosing Institution	CBSA	-	-	-	-	-	(2)	-	-	-	-	-	-	-	-	(2)	-	(4)
	GAC	-	-	-	-	(1)	41 (12)	-	-	-	-	-	-	-	-	7 (2)	-	49 (15)
	IRCC	-	-	-	-	76	770	-	-	-	-	-	-	-	-	(1)	-	847 (1)
	TOTAL (proactive)	-	-	-	-	77 (1)	813 (14)	-	-	-	-	-	-	-	-	10 (5)	-	900 (20)

16. This substantial increase in records was primarily driven by IRCC's disclosures to CSIS, which grew nearly 300% from 194 in 2023 to 770 in 2024. IRCC previously disclosed similar information to CSIS under the *Privacy Act*, whereas now the SCIDA is the primary mechanism for CSIS to obtain immigration information. CSIS also credits the increase in disclosures to enhanced collaboration with IRCC aimed at improving operational staff awareness and understanding of the SCIDA regime.
17. As observed in prior years, institutions predominantly made disclosures following a request. Only 2% of disclosures were sent proactively by the disclosing institution.

Record Keeping Requirements – Section 9

Finding 2. NSIRA found that, within the sample of disclosures reviewed, every institution that disclosed or received information pursuant to the SCIDA in 2024 generally complied with its record-keeping obligations under section 9.

18. Section 9 of the SCIDA establishes record-keeping obligations for both disclosing and recipient institutions. These requirements are designed to promote accountability and transparency by mandating the documentation of essential information, including descriptions of the disclosed or received data, the individuals involved, relevant dates, and the legal basis for the disclosure. Institutions are also required to record whether the information was destroyed or returned.
19. NSIRA's analysis of records submitted by CSIS and IRCC revealed several minor discrepancies in record-keeping. These discrepancies can be attributed to duplicated, amended, and cancelled requests from CSIS. For example, in some cases, follow-up questions from CSIS regarding disclosures it had received were recorded by IRCC as a different request.
20. In addition, IRCC assigned sequential file numbers for a number of requests that were sent in 2024, but not processed until 2025. These disclosures were included in the record-keeping logs submitted to NSIRA. IRCC explained that, moving forward, it will only assign file numbers to requests that are completed in the current calendar year to minimize confusion.
21. IRCC also noted that it has committed to sharing its record-keeping log with CSIS on a quarterly basis to address potential discrepancies early. Clear and effective communication between disclosing and recipient institutions is vital to accurate record-keeping and enables secure information management, legal compliance, and administrative precision.

Information Sharing Agreements – Subsection 4(c)

Finding 3. NSIRA found that CSE provided IRCC with more information than necessary in three of its requests for disclosure under the SCIDA.

22. In August 2023, CSE and IRCC signed an information sharing agreement (ISA) to formalize their regular information exchanges and facilitate compliance with the SCIDA. The primary purpose of IRCC disclosures to CSE under the SCIDA is to determine a subject of interest’s legal citizenship status and/or immigration status in Canada. These disclosures help to ensure CSE’s lawfulness, as its mandate prohibits the direction of operational activities at Canadians and persons in Canada.
23. In its requests, CSE provides an individual’s identifying information in order for IRCC to conduct a search in the relevant systems, primarily the Global Case Management System (GCMS). The GCMS holds all citizenship and immigration information of Canadian citizens, foreign nationals, and permanent residents. It includes any application submitted by individuals as well as information entered by immigration officers and/or other departments, such as the CBSA.
24. At minimum, CSE provides IRCC with an individual’s full name and date of birth in its request. When available, CSE may include additional identifying information such as an individual’s known or suspected nationality, place of birth, and phone number(s), among others. The ISA between CSE and IRCC contains a comprehensive list of all the information that CSE may provide to assist IRCC in producing accurate results.
25. In three different instances, however, NSIRA observed that CSE provided IRCC with additional personal information that was not identified in the ISA. CSE explained that all relevant details were disclosed to increase the likelihood of IRCC yielding results. IRCC confirmed to NSIRA that it could not, and has never, leveraged the specific personal information provided by CSE to conduct its searches.
26. The ISA does not formally prohibit CSE from sharing information outside of the parameters agreed upon with IRCC. Nevertheless, CSE should verify whether the information it shares is relevant to the disclosing institution to avoid unnecessary sharing of personal data.

Recommendation 1. NSIRA recommends that CSE limit the sharing of information when requesting a disclosure under the SCIDA to only that which IRCC has identified as relevant to its information holdings.

Disclosure of Information Requirements – Section 5

Finding 4. NSIRA found that IRCC and CSIS’s implementation of a tiered request and disclosure process reduced the amount of third-party information disclosed by IRCC, which contributed to enhanced compliance with the SCIDA.

27. In the spring of 2024, IRCC and CSIS developed a tiered process for sharing under the SCIDA and introduced the classification of SCIDA requests and disclosures into “basic” or “advanced”.³ In implementing this process, IRCC and CSIS also formally adopted three standardized templates: a request letter, a checklist, and a response form. The checklist and response forms, in particular, aim to guide IRCC analysts in providing only necessary information and were included in all disclosures.
28. At minimum, a basic disclosure contains biographic details from the past five years, such as citizenship or immigration information, marital status, and contact information. It may also include photographs, recent employment information, travel history, and physical characteristics.
29. Should CSIS require an extensive personal history and supporting documents, such as scanned immigration applications, the request becomes an advanced SCIDA disclosure requiring additional rationale. This type of disclosure often contains information from a longer period of time (past ten years or more).
30. Previously, in order to share even basic biographic information, IRCC would include a scanned copy of an individual’s most recent immigration application (e.g. a passport or visa application). As a result, a number of disclosures from early in the review year contained third party information, such as unredacted guarantor, emergency contact, or reference information. NSIRA observed that the tiered system reduced the number of instances where IRCC included third party information in a basic SCIDA disclosure, in part because scanned copies of applications were no longer included.
31. Typically, IRCC will redact references from passport applications in an advanced disclosure. Other types of third-party information are redacted on a case-by-case basis.
32. The disclosure process begins when IRCC receives a request letter from CSIS containing a standardized list of items agreed upon by both institutions. This approach allows CSIS to identify only the information necessary for its request, addressing previous issues with customized and inconsistent information lists. For

³ Although not reviewed by NSIRA, disclosures based on images provided by CSIS were also treated as a separate category by IRCC.

example, CSIS may request biographic details, such as citizenship and passport information, but choose not to request contact information. Advanced request letters include an option to receive scanned copies of applications.

33. Throughout 2024, the request letter, checklist, and response form evolved to meet the needs of IRCC and CSIS. NSIRA observed that new types of commonly requested information that had been previously absent from the request letter would be added as needed. In addition, IRCC combined the checklist and response form to reduce its administrative burden. The tiered process enabled IRCC to manage the increase in disclosures while limiting the amount of third-party information shared.
34. Importantly, IRCC's decision to use a response checklist and form indicates an iterative process that improved the operational efficiency and legal compliance of both institutions under the SCIDA. Specific response times are prioritized into the following three categories: urgent life-threatening requests, priority operational requests, and routine requests. IRCC intends to prioritize requests from other institutions under the SCIDA in a similar manner.
35. The disclosures below briefly illustrate how the tiered process improved IRCC's minimization of personal information in disclosures under the SCIDA. The first case represents a typical disclosure prior to the tiered system, while the second and third disclosures occurred after its introduction.

Disclosure 1

36. CSIS sent a letter to IRCC requesting⁴ the disclosure of information about a foreign individual under investigation relating to a particular institution. The request was to include records from the past five years.
37. Without a system to limit what information was shared, IRCC disclosed all available scanned copies of the individual's study permit, work permit, permanent residence, and temporary resident visa applications. All documents provided in the disclosure were without redactions and included third party, minor, and financial information.

Disclosure 2

⁴ The request included, but was not limited to, the following: personal information (marital status, photograph(s), status in Canada, details of employment history), contact information (current and past home addresses, telephone and email addresses), information on associates (references, emergency contact(s), and guarantor(s)), and passport information.

38. CSIS requested⁵ a basic SCIDA disclosure from IRCC for information relating to individuals affiliated with a particular foreign entity. In its justification, CSIS noted that the foreign entity and any individuals identified were of “national security interest” in relation to a CSIS investigation.
39. As this was a basic request, IRCC took steps towards limiting the disclosure by providing CSIS with a chart containing only the name, place and date of birth, status or immigration history, and the nature of affiliation. In email correspondence, IRCC stated that should CSIS require additional details or would like to request an advanced SCIDA for any or all of the individuals implicated, it would be required to include an additional detailed rationale.

Disclosure 3

40. CSIS requested⁶ an advanced disclosure from IRCC for information relating to several individuals with the justification that it had “reasonable grounds to believe” the subjects may have been in contact with “known members” of a foreign intelligence service. CSIS continued to justify its reasoning in detail, providing IRCC with a substantial amount of contextual information about the foreign entity in question and how the information it requested would contribute to its investigation.
41. CSIS also requested scanned copies of all documents in its request. IRCC disclosed nearly all categories of information requested by CSIS. In the checklist attached to the disclosure, IRCC stated that it had redacted third party information as well as other records that were irrelevant to CSIS’s request.
42. When compared to the first case, the delineation of basic and advanced disclosures under the SCIDA prevented the over sharing of personal information by IRCC in the second case without further justification. Despite CSIS’s expanded justification in the third case, IRCC did not include all the information in its holdings on the identified subjects because not everything was relevant.

⁵ For any individuals IRCC identified, CSIS requested the following: Personal information (biographic features, marital status, photographs, status in Canada), as well as citizenship, passport, and contact information (phone number(s), email address(es), and residential addresses).

⁶ CSIS requested the following: Personal information (biographic features, marital status, photographs, details of employment history) as well as all relevant immigration, citizenship, and passport information. CSIS also requested contact information (phone number(s), email address(es), residential addresses).

Contribution and Proportionality Tests – Section 5(1)

Finding 5. NSIRA found instances when the information provided to IRCC by CSIS was limited and hampered IRCC’s ability to fulfill its obligation as a disclosing institution to satisfy itself that the information disclosed is in respect of an activity that undermines the security of Canada.

43. SCIDA disclosures made under section 5(1) require IRCC to satisfy itself of two specific criteria. First, IRCC must satisfy itself that the disclosure will contribute to CSIS’s exercise of its jurisdiction in respect of activities that undermine the security of Canada. Second, IRCC must satisfy itself that the disclosure will not affect any person’s privacy interest more than is reasonably necessary in the circumstances. If IRCC is satisfied in both instances, it “may” make a disclosure. The onus is on the disclosing institution to assure itself that the information it discloses will contribute in the requisite sense.
44. While CSIS may not be required to share detailed information about its investigations, programs, or activities with IRCC, it needs to provide enough information in a request so that IRCC can responsibly exercise its discretion. A succinct high-level explanation of the link between the information sought and CSIS’s national security jurisdiction and responsibilities may be enough. However, disclosing institutions can seek clarification by requiring a more specific articulation of the activity that undermines the security of Canada that the request relates to.
45. In the majority of basic requests reviewed by NSIRA, CSIS elected to use scant phrasing in its justifications, such as “Subject is of national security interest in relation to the Service’s investigation of” the threat in question. In contrast, NSIRA observed other basic requests where CSIS demonstrated how the requested information would contribute to its investigations in a clear and descriptive manner in its justification. As a matter of course, advanced requests almost always contained robust justifications.
46. Inconsistencies in the description of the undermining activity in CSIS’s basic request letters did not often prompt IRCC to seek further clarification. In practice, IRCC maintained an institutional understanding that CSIS would only request information that will contribute to its mandate. NSIRA did not observe that IRCC conducted independent assessments based on a structured framework or consistent criteria.
47. IRCC has stated that it redacts any information it deems irrelevant in its disclosures to ensure that only pertinent details are disclosed. Particularly for advanced and bulk requests, IRCC was not always satisfied with CSIS’s justifications. NSIRA observed

that IRCC either required additional rationale, disclosed less information than had been requested, or redacted unnecessary third-party information.

48. The absence of detailed justifications in SCIDA requests risks compromising compliance with paragraph 5(1)(b). Consequently, recipient institutions should provide disclosing institutions with the necessary information and rationale to satisfy the disclosing institution's contribution threshold. A sufficient analysis of the activity that undermines the security of Canada requires that IRCC have knowledge of those circumstances.
49. The recommendation below echoes those from NSIRA's 2024 review of the SCIDA, namely that IRCC should not automatically accept, without an independent assessment, a recipient institution's request. The review also recommended that IRCC disclose only the minimum information reasonably necessary to protect individuals' privacy in the circumstances and comply with the legal standards of the SCIDA.⁷

Recommendation 2. NSIRA recommends that IRCC seek clarification from requesting institutions, as needed, to ensure it has all relevant information necessary to fulfill its obligations as a disclosing institution under the SCIDA, before making a disclosure.

Finding 6. NSIRA found that IRCC did not have a policy governing the disclosure of information concerning minors under the SCIDA.

50. In 2024, IRCC indicated that it had received an increase in requests for disclosures regarding minors and engaged with CSIS to ensure their privacy. IRCC's existing SCIDA policy, however, does not address the treatment of minors in disclosures under the regime.
51. NSIRA observed that IRCC was inconsistent in its approach to disclosing information about minors and did not redact information appropriately in several disclosures reviewed. In at least one instance, IRCC stated that it had redacted a minor's information. However, NSIRA observed that IRCC had done so inconsistently, leaving the minor's name, date of birth, and national identification number unredacted elsewhere in the same disclosure. In other disclosures, IRCC either redacted information about a minor in full or chose not to make the disclosure at all.
52. The care attendant to a minor's privacy rights in other areas of the law (as seen in, among others, the *Criminal Code*, the *Youth Criminal Justice Act* and various

⁷ NSIRA Review 23-11 at recommendation 2 and 3.

international conventions) indicates that minors may also attract a heightened privacy expectation in a national security context. Children under 16, for example, may not have a choice in submitting applications for passports which are completed on their behalf by a parent or guardian.

Recommendation 3. NSIRA recommends that IRCC institute a policy on the disclosure of information related to minors that recognizes their distinct privacy interests.

Requirement to Destroy or Return – Subsection 5.1(1)

Finding 7. NSIRA found that CSIS may not have complied with subsection 5.1(1) of the SCIDA when it retained one disclosure containing personal information that was not necessary for exercising its jurisdiction.

53. Subsection 5.1(1) of the SCIDA requires, as soon as feasible, the destruction or return of any personal information received under section 5 of the Act that is not necessary for a department to fulfill their lawful responsibilities related to national security. CSIS is excluded from this requirement by subsection 5.1(3) when a disclosure is retained pursuant to the performance of its duties and functions under section 12 of the CSIS Act.
54. In 2024, CSIS was the only institution to identify disclosures containing information that was destroyed or returned under subsection 5.1(1): three were deemed non-reportable, one was incorrect (wrong subject), and one had been disclosed by IRCC before CSIS could cancel the request, although it was not disseminated.
55. Separately, NSIRA identified one disclosure where CSIS retained personal information about the wrong individual. In early 2024, CSIS sent a letter to IRCC requesting⁸ a foreign citizen's current and past applications for the past five years. As the request was made before the tiered process had been implemented, IRCC's disclosure was extensive and included full visa and work permit applications, as well as unredacted familial and financial information.
56. Shortly following receipt of the disclosure, CSIS assessed that the individual implicated was not the subject of the request. Despite the requirement to destroy the

⁸ The request included, but was not limited to, the following: personal information (marital status, photograph(s), status in Canada, details of employment history), contact information (current and past home addresses, telephone and email addresses), information on associates (references, emergency contact(s), and guarantor(s)), and passport information.

information, CSIS retained it in its entirety for “reference purposes.” When asked, CSIS confirmed the disclosure should not have been retained “in its totality and possibly at all” and that the matter had been referred to its internal compliance section.

57. To the extent that it is strictly necessary, section 12 of the CSIS Act allows CSIS to collect, analyse and retain on activities constituting threats to the security of Canada. However, as CSIS did not claim that this information was retained pursuant to section 12 of the CSIS Act, and thus was not strictly necessary to keep, the exception at 5.1(3) of the SCIDA did not apply and CSIS was required to destroy or return the information pursuant to 5.1(1).

Recommendation 4. NSIRA recommends that CSIS destroy all personal information in one disclosure that was not necessary for exercising its jurisdiction.

IV. Conclusion

58. This review marks the sixth year that NSIRA has examined GC institutions’ compliance with the SCIDA. NSIRA concluded that, within the disclosures reviewed, institutions generally adhered to the SCIDA’s requirements for disclosure and record-keeping.
59. NSIRA noted important improvements that streamlined the request and disclosure process between IRCC and CSIS and enhanced compliance. However, NSIRA observed risks with IRCC’s application of the substantive requirements under paragraphs 5(1)(a) and 5(1)(b) of the SCIDA.
60. NSIRA also identified possible non-compliance with subsection 5.1(1) of the SCIDA owing to CSIS’s retention of personal information that it had identified as unnecessary.
61. NSIRA’s recommendations in this review are designed to assist both recipient and disclosing institutions in adhering to the SCIDA’s privacy standards while effectively supporting national security and lawful mandates.

Annex A. Historical SCIDA Disclosures

Disclosing Institution ⁹		Designated Recipient Institutions under the SCIDA, Schedule 3															TOTAL
		CBSA	CFIA	CNSC	CRA	CSE	CSIS	DND/CA	Finance	FINTRAC	GAC	Health	IRCC	PHAC	PS	RCMP	
2023	CBSA	-	-	-	-	-	-	-	-	-	-	-	-	-	2 (2)	-	2 (2)
	GAC	-	-	-	-	1 (1)	10 (0)	-	-	-	-	-	-	-	-	-	15 (1)
	IRCC	-	-	-	-	58 (0)	194 (7)	-	-	-	-	-	-	-	-	-	252 (7)
	TOTAL (proactive)	-	-	-	-	59 (1)	204 (7)	-	-	-	-	-	-	-	6 (2)	-	269 (10)
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 Institutions 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 B. Findings and Recommendations

NSIRA made the following findings and recommendations in this review:

Volume and Trend Analysis

Finding 1. NSIRA found that IRCC's disclosures to CSIS under the SCIDA increased significantly in 2024.

Record Keeping Requirements – Section 9

Finding 2. NSIRA found that, within the sample of disclosures reviewed, every institution that disclosed or received information pursuant to the SCIDA in 2024 generally complied with its record-keeping obligations under section 9.

Information Sharing Agreements – Subsection 4(c)

Finding 3. NSIRA found that CSE provided IRCC with more information than necessary in three of its requests for disclosure under the SCIDA.

Recommendation 1. NSIRA recommends that CSE limit the sharing of information when requesting a disclosure under the SCIDA to only that which IRCC has identified as relevant to its information holdings.

Disclosure of Information Requirements – Section 5

Finding 4. NSIRA found that IRCC and CSIS's implementation of a tiered request and disclosure process reduced the amount of third-party information disclosed by IRCC, which contributed to enhanced compliance with the SCIDA.

Finding 5. NSIRA found instances when the information provided to IRCC by CSIS was limited and hampered IRCC's ability to fulfill its obligation as a disclosing institution to satisfy itself that the information disclosed is in respect of an activity that undermines the security of Canada.

Recommendation 2. NSIRA recommends that IRCC seek clarification from requesting institutions, as needed, to ensure it has all relevant information necessary to fulfill its obligations as a disclosing institution under the SCIDA, before making a disclosure.

Finding 6. NSIRA found that IRCC did not have a policy governing the disclosure of information concerning minors under the SCIDA.

Recommendation 3. NSIRA recommends that IRCC institute a policy on the disclosure of information related to minors that recognizes their distinct privacy interests.

Requirement to Destroy or Return – Subsection 5.1(1)

Finding 7. NSIRA found that CSIS may not have complied with subsection 5.1(1) of the SCIDA when it retained one disclosure containing personal information that was not necessary for exercising its jurisdiction.

Recommendation 4. NSIRA recommends that CSIS destroy all personal information in one disclosure that was not necessary for exercising its jurisdiction.