National Security and Intelligence Review Agency

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

REVIEW OF FEDERAL INSTITUTIONS' DISCLOSURES OF INFORMATION UNDER *THE SECURITY OF CANADA INFORMATION DISCLOSURE ACT* IN 2021

Table of Contents

1. EXECUTIVE SUMMARY 3
2. INTRODUCTION 4
Focus of this Review 5
Review Objectives 6
Methodology 7
3. ANALYSIS 7
Thresholds for disclosing information to federal institutions under the SCIDA 8
a) Jurisdiction or responsibilities in respect of activities that undermine the security of Canada 8
b) Privacy interest not impacted more than reasonably necessary in the circumstances. 12
Accuracy and Reliability Statements 14
Record-keeping 15
Training on the SCIDA 16
4. RESPONSIVENESS AND PROVISION OF INFORMATION 18
5. CONCLUSION 18
ANNEX A. SCIDA BACKGROUND 19
Air India Inquiry 19
Arar Inquiry 20
Government Response: The SCISA 23
The SCIDA 23
ANNEX B. SCIDA BY THE NUMBERS 26
Total Disclosures under the SCIDA 26
Total Proactive Disclosures 26
Proactive Disclosures by GAC 27
ANNEX C. SECURITY OF CANADA INFORMATION DISCLOSURE ACT (SCIDA) LEGAL FRAMEWORK 28
Federal institutions that can receive information under the SCIDA 28
ANNEX D. FINDINGS AND RECOMMENDATIONS 31
Findings 31
Recommendations 32

1. EXECUTIVE SUMMARY

1. This report describes the results of a review by the National Security and Intelligence Review Agency (NSIRA) of the 2021 disclosures made by federal institutions under the *Security of Canada Information Disclosure Act* (SCIDA)[1]. This is the third year of implementation of the SCIDA regime. This year, NSIRA decided to focus the review on Global Affairs Canada's (GAC) proactive disclosures.

2. The SCIDA encourages and facilitates the disclosure of information between federal institutions to protect Canada against activities that undermine or threaten national security, subject to certain conditions. The SCIDA provides a two-part threshold which must be met prior to making a disclosure: 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,[2] and will not affect any person's privacy interest more than reasonably necessary in the circumstances.[3] The SCIDA also includes provisions and guiding principles related to the management of disclosures, including accuracy and reliability statements and record keeping obligations.

3. NSIRA identified concerns that demonstrate the need for improved training. NSIRA found that there is potential for confusion on whether the SCIDA is the appropriate mechanism for certain disclosures of national security-related information. Some disclosures were of concern as GAC did not meet the two-part threshold requirements of the SCIDA prior to disclosing the information. Without meeting these requirements, some disclosures of personal information were not compliant with the SCIDA. Two disclosures did not contain accuracy and reliability statements, as required under the SCIDA. With respect to record-keeping, NSIRA recommends that departments contemporaneously document the information relied on to satisfy themselves that disclosures will not affect any person's privacy interest more than is reasonably necessary in the circumstances.[4]

4. NSIRA is confident that it received all information necessary to conduct the review.

---

[1] *Security of Canada Information Disclosure Act*, S.C. 2015, c. 20, s. 2, [SCIDA] https://laws.justice.gc.ca/eng/acts/S-6.9/. SCIDA came into force on 21 June 2019. SCIDA's predecessor, the *Security of Canada Information Sharing Act*, was in force from 1 August 2015 to 20 June 2019.

[2] SCIDA, para. 5(1)(a)

[3] SCIDA, para. 5(1)(b)

[4] SCIDA, para. 9(1)(e)

2. INTRODUCTION

5. When federal departments fail to share national security information in a timely, coordinated, or responsible manner, serious and tragic consequences can result – as the Arar and Air India Inquiries found.[5] As a mechanism in Canada's national security accountability framework, NSIRA is mandated to prepare a report respecting disclosures under the *Security of Canada Information Disclosure Act* (SCIDA) during the previous calendar year.[6] This is the only NSIRA review that must be made public and laid before both the House of Commons and the Senate,[7] reflecting the importance Parliament has placed on independent review and accountability of national security information disclosure.

6. The SCIDA's designated long title also reflects its stated purpose: *An Act to encourage and facilitate the disclosure of information between Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada*.[8]

7. The SCIDA governs how Government of Canada institutions[9] disclose information, including personal information, that is relevant to activities that undermine the security of Canada, to a select group of federal institutions with national security mandates. Disclosures are either made proactively, on the initiative of a Government of Canada institution, or in response to a request by an institution authorized to receive information under the SCIDA.

8. It is important to note that the SCIDA is simply a tool. It is only as useful as its real-time recognition and application. Its success relies on how individuals and institutions interact with

---

[5] Canada, Air India Review Secretariat, *Lessons to be Learned: The report of the Honourable Bob Rae, Independent Advisor to the Minister of Public Safety and Emergency Preparedness, on outstanding questions with respect to the bombing of Air India Flight 182*, by Bob Rae, (Ottawa: Air India Review Secretariat, 2005) at 23. See also Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar – Analysis and Recommendations*, (Ottawa: Public Works and Government Services Canada, 2006) at 331. For a full discussion of the development of the SCIDA, see Annex A, Background.

[6] *National Security and Intelligence Review Agency Act*, SC 2019, c 13, s 2 (NSIRA Act), ss. 39(1).

[7] NSIRA Act, ss. 39(2).

[8] See also *Security of Canada Information Disclosure Act*, SC 2015, c 20, s 2, s 3.

[9] The term "Government of Canada institution" is defined by linking to the definition of the same term in the *Privacy Act*, subject to any exclusions listed in Schedule 1 of the SCIDA. See SCIDA, ss. 2(1).

and implement its provisions. Those federal government institutions authorized to disclose information under the SCIDA must maintain a certain vigilance for information that may have national security repercussions, including at the most basic operational level. Having recognized information that could involve national security matters, departments must then decide whether they are authorized to disclose that information and to whom, paying close attention to minimizing any impacts on individual privacy rights.

9. Federal departments and agencies with core national security mandates are generally able to rely on their own legal frameworks to share information with other domestic institutions, and do not require the SCIDA to do so. Previous NSIRA reports have found that for many such institutions, disclosures made under the SCIDA comprise only a small portion of their domestic national security information sharing.[10]

10. NSIRA understands the significance of the SCIDA in the overall national security framework, and is concerned with its robust application, in keeping with the provisions of the SCIDA, including its guiding principles, and with respect to the disclosure of personal information. What is more, NSIRA has the ability to review all disclosures across the Government of Canada, and through this broad lens, can identify common themes and trends. This perspective, not available to individual federal departments, enables NSIRA to make findings and recommendations that can strengthen overall information disclosure within the national security framework.

Focus of this Review

11. In determining the focus of this review, NSIRA considered the concerns raised in its review conducted the year prior. In the review of disclosures made under the SCIDA in 2020, which NSIRA undertook jointly with the Office of the Privacy Commissioner (OPC), the review found that the majority of federal department disclosures – approximately 99 per cent – met the threshold requirements that permit information to be disclosed under the SCIDA. In other words, the disclosing institutions sufficiently demonstrated that they had satisfied themselves, prior to providing the disclosures, that the information to be disclosed would contribute to the exercise of the recipient's jurisdiction or responsibilities respecting activities that undermine the security of Canada, and that it would not affect any person's privacy interest more than reasonably necessary in the circumstances.

[10] See NSIRA and the OPC's Review of federal institutions' disclosures under the *Security of Canada information Disclosure Act* in 2020 (SCIDA 2020 Review), p. 18.

12. The few disclosures that raised concerns, however, were those that had been provided to the recipient institutions on a proactive basis.[11] As such, NSIRA chose to focus on this category for its 2021 review of disclosures under the SCIDA. In 2021, the majority of proactive disclosures came from Global Affairs Canada (GAC). NSIRA therefore chose to focus on GAC's proactive disclosures in 2021, as a representative sample.

13. In addition to reviewing these disclosures from the perspective of the SCIDA's prerequisite thresholds, this review also assessed other important requirements under the SCIDA that help to ensure responsible disclosures of national security information. These include the need for disclosures to be accompanied by statements that attest to the accuracy and reliability of the information being disclosed, as well as the obligation on all disclosing institutions to prepare and keep records that set out a description of the information that was relied on to satisfy themselves that the disclosure was authorized under the SCIDA.

14. Although the review sample focused on GAC proactive disclosures, many findings and recommendations are general and illustrative and, in many instances, may be useful to all institutions when disclosing under the SCIDA.

Review Objectives

15. The objectives of this review were to assess proactive disclosures of information under the SCIDA.

16. Specifically, the review assessed whether GAC:

a) Satisfied itself, prior to disclosing any information, that the disclosure would contribute to the exercise of the recipient institution's jurisdiction, or the carrying out of its responsibilities, in respect of activities that undermine the security of Canada, as required under paragraph 5(1)(a) of the SCIDA;
b) Satisfied itself, prior to disclosing any information, that the disclosure would not affect any person's privacy interest more than reasonably necessary in the circumstances, as required under paragraph 5(1)(b) of the SCIDA;
c) Described, at the time of the disclosure, the accuracy of the information disclosed and the reliability of the manner in which it was obtained, as required under subsection 5(2) of the SCIDA; and

[11] SCIDA 2020 Review, p. 5.

d) Kept records that included a description of the information that was relied on to satisfy itself that the disclosure was authorized under the SCIDA, as required under paragraph 9(1)(e) of the SCIDA.

Methodology

17. NSIRA received 195 disclosures of information from federal departments that reported either disclosing or receiving information under the SCIDA between January 1, 2021 and December 31, 2021. NSIRA conducted a preliminary review of all disclosures received.[12]

18. NSIRA focused this year's review on GAC proactive disclosures only. GAC identified 16 proactive disclosures out of a total of 44 disclosures under the SCIDA in 2021. However, in reviewing the material provided by GAC, NSIRA noted that three of these files were in fact requests for information from another department, and not disclosures of information under the SCIDA. As such, NSIRA removed these three files from the review sample, and only analyzed the remaining 13 disclosures identified by GAC as proactive disclosures.

19. NSIRA sent five follow up requests for information to GAC regarding its disclosures, and assessed all records provided.

3. ANALYSIS

20. In conducting this review, NSIRA observed positive components of disclosures that it endeavours to highlight in this report. Proactive disclosures are an important feature of the SCIDA regime, and the following findings and recommendations aim to enhance compliance with the SCIDA.

[12] See Annex B for a breakdown of SCIDA disclosures in 2021.

Thresholds for disclosing information to federal institutions under the SCIDA

a) Jurisdiction or responsibilities in respect of activities that undermine the security of Canada

21. Paragraph 5(1)(a) of the SCIDA requires departments to satisfy themselves that disclosures "will contribute to the exercise of the recipient institution's jurisdiction, or the carrying out of its responsibilities, under an Act of Parliament or another lawful authority, in respect of activities that undermine the security of Canada."

22. The definition of "activity that undermines the security of Canada" is set out at subsection 2(1) of the SCIDA and includes, for example, espionage and terrorism. Certain activities are excluded from this definition, notably advocacy and protest not carried out in conjunction with an activity that undermines the security of Canada.

23. In conducting this review, NSIRA examined each disclosure in the sample and its corresponding documentation to assess whether GAC had satisfied itself, prior to making the disclosure, that the information to be disclosed would contribute to the recipient department's jurisdiction in respect of activities that undermine the security of Canada, as defined in the SCIDA.

24. In 12 of the 13 disclosures reviewed, GAC sufficiently demonstrated that it had satisfied itself as to these requirements. Furthermore, in all of these 12 disclosures, GAC documented that it had considered not only whether the recipient had the appropriate jurisdiction, but also how the information would contribute to that jurisdiction in respect of an activity that undermines the security of Canada as defined in the SCIDA. For example, see text box 1. The information in the disclosure file supports the text of this statement.

Text box 1: Example of statement in disclosure demonstrating GAC satisfied itself as to the requirements under 5(1)(a) of the SCIDA[13]

GAC's disclosure will contribute to the carrying out of CSIS' responsibilities under section 12 of the CSIS Act, which require CSIS to investigate activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. Section 2.a of the CSIS Act defines threats to the security of Canada as encompassing threats or acts of "espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage." CSIS collects, analyzes and retains information and intelligence on these threats to the extent that it is strictly necessary to do so, and reports to and advises the Government of Canada. In the circumstances, GAC's disclosure will contribute to CSIS' responsibility under section 12 of the CSIS Act to investigate and report on threats to the security of Canada as defined in section 2.a of the CSIS Act. Specifically, the disclosure will contribute to an assessment of a potential espionage threat [against Canadian interests abroad].

25. However, NSIRA observed that in one of those twelve disclosures, GAC consulted on more information than necessary to determine whether the disclosure was authorized under the SCIDA. This disclosure is described below.

Disclosure 1

26. A foreign country provided information about an individual with ties to Canada, to GAC headquarters, and requested that GAC forward the information to appropriate authorities. GAC then met with CSIS and showed them the information in their holdings, in order to clarify whether the information contributed to CSIS's national security mandate. CSIS reviewed the information and confirmed that the information was of value to their investigation. CSIS did not report any of the information in its holdings.

27. Following that consultation, GAC concluded that a number of the documents did not pertain to an activity that undermines the security of Canada, as they contained "significant amounts of personal information unrelated to [the subject of the investigation] and reflecting acts considered lawful in Canada, such as freedom of speech (with no stated intent to engage in acts of violence) and freedom of peaceful assembly." As such, GAC subsequently formally disclosed to CSIS only a fraction of the previously consulted documents. With respect to this formal

[13] Information in square brackets in this report has been altered by NSIRA to protect injurious information.

disclosure, GAC demonstrated that it satisfied itself as to the requirements under paragraph 5(1)(a) of the SCIDA.

28. GAC indicated to NSIRA that the Public Safety guide on responsible information-sharing (PS Guide)[14] is its primary policy guidance on the SCIDA. NSIRA notes that the PS Guide encourages government institutions to "communicate with the designated recipient institution prior to disclosure to determine not only whether the information is linked to activities that undermine the security of Canada but also how it contributed to that institution's national security mandate."[15] This should not be interpreted as providing authorization to consult on more information than necessary, given the possibility that information outside the scope of a SCIDA disclosure may be included.

29. During its consultation with CSIS, GAC consulted on information that it later assessed as not concerning an activity that undermines the security of Canada as defined in the SCIDA and which was later removed from the formal disclosure under the SCIDA. The consultation involved showing GAC's full information holdings to CSIS, which was more information than necessary to obtain confirmation from CSIS that the information was of value. Information used in consultations should be limited to the information necessary to obtain confirmation from the potential recipient that the information contributes to the carrying-out of its mandate and is linked to activities that undermine the security of Canada.

30. Furthermore, despite twelve out of thirteen disclosures meeting the requirements of paragraph 5(1)(a) of the SCIDA, one disclosure did not. NSIRA addresses this disclosure below.

Disclosure 2

31. An individual overseas, on their own initiative, identified themselves as a member of that country's government and provided information to an official at a Canadian embassy about an alleged threat. GAC disclosed this information along with personal information, including the individual's contact information, to the Canadian Security Intelligence Service (CSIS), invoking the SCIDA as an authority to make the disclosure. However, GAC did not consider whether this disclosure met the two threshold requirements under paragraphs 5(1)(a) and 5(1)(b) of the SCIDA, prior to disclosing this information in its entirety. During the course of this review, GAC explained to NSIRA that the disclosure was erroneously made under the SCIDA, and it was authorized under

[14] *Security of Canada Information Disclosure Act – A Step-by-Step Guide to Responsible Information Sharing* (December 2019) (PS Guide)

[15] PS Guide, page 17

another authority for disclosing information in such circumstances, that is the *Privacy Act* or the Crown Prerogative. NSIRA did not assess whether these mechanisms would have been appropriate in the circumstances. Nonetheless this example demonstrates a) that there is potential for confusion on whether the SCIDA is the appropriate mechanism for certain disclosures of national security-related information, and b) that such confusion, in this case, led to the improper use of the SCIDA to disclose.

Finding no. 1: NSIRA finds that, in twelve out of thirteen disclosures, GAC demonstrated that it satisfied itself as to the contribution of the information to the recipient institution's responsibilities in respect of activities that undermine the security of Canada, as required under paragraph 5(1)(a) of the SCIDA.

Finding no. 2: NSIRA finds that, without first conducting the analysis under paragraph 5(1)(a) of the SCIDA, departments risk disclosing information that does not pertain to the national security mandate of the recipient institution or to activities that undermine the security of Canada.

Finding no. 3: NSIRA finds that, in one of thirteen disclosures, GAC consulted on more information than necessary to obtain confirmation that the disclosure contributed to CSIS's mandate and was linked to activities that undermine the security of Canada.

Recommendation no. 1: NSIRA recommends that consultations be limited to the information necessary to obtain confirmation from the potential recipient that the information contributes to its mandate and is linked to activities that undermine the security of Canada.

b) Privacy interest not impacted more than reasonably necessary in the circumstances

32. Paragraph 5(1)(b) of the SCIDA requires that disclosing institutions be satisfied that the disclosure will not affect any person's privacy interests more than reasonably necessary in the circumstances.

33. All thirteen proactive disclosures included personal information as defined in the *Privacy Act*[16], that is, identifiable information about an individual, such as name, contact information, background information, or suspicions concerning the individual.

34. The PS Guide provides direction on the type of analysis required prior to disclosing personal information. More specifically, the PS Guide states "whether the information impacting a person's privacy interest is considered 'reasonably necessary' will depend upon the particular circumstances of each case. Relevant considerations may include contextual factors, such as the type and nature of the information in question and the particular purpose for the disclosure."[17]

35. In response to NSIRA requests for further information, GAC explained how it satisfied itself that these proactive disclosures did not affect any person's privacy interest more than reasonably necessary in the circumstances.

36. For example, GAC explained that in eight of the thirteen disclosures, GAC determined that some of the information it was considering disclosing was not within the scope of the recipient institution's mandate. In the same disclosures, GAC also stated that it determined that some of the information in its holdings did not contribute to the institution's investigation or fall within the recipient institution's original request for information. For example, in one disclosure, only an individual's travel status abroad was shared with CSIS as this pertained to the latter's responsibilities in a national security matter. Other information in GAC's holdings, such as information concerning other individuals, was determined by GAC not to be relevant, and therefore was not included in the disclosure.

37. Similarly, GAC explained that in two of the thirteen disclosures, GAC determined that some information was necessary to report to the recipient department, and therefore included in the disclosure. More detailed information not linked to activities that undermine the safety of Canada was not disclosed. For example, in one of the two disclosures, only information about suspected

[16] *Privacy Act*, R.S.C., 1985, c. P-21

[17] PS Guide, page 18.

espionage activity was disclosed to CSIS, while detailed information about certain personal activities and behaviours was withheld.

38. NSIRA observed that of the 13 disclosures in the sample, three disclosures did not meet the requirements under paragraph 5(1)(b) of the SCIDA.

39. In Disclosure 2, described above, GAC disclosed information that was received from an individual who, on their own initiative, provided information to an official at a Canadian embassy overseas. GAC did not conduct any analysis under the SCIDA including whether the disclosure would affect privacy interests more than reasonably necessary in the circumstances, and proceeded with disclosing the entirety of the information to CSIS. GAC explained to NSIRA that the disclosure was erroneously made under the SCIDA, and was authorized under another authority for disclosing information, that is the *Privacy Act* or the Crown Prerogative. NSIRA did not assess whether these mechanisms would have been appropriate in the circumstances.

Disclosures 3 and 4

40. A Canadian embassy abroad received screen shots of a private social media group. The screenshots included information about a political movement in a foreign country. They also contained the contact information of all members of the group. While the group shared posters about the movement and information concerning protests in Canada, there were no threats, whether specific or general, in the material. However, based on some information in the screenshots, as well as the broader context of protests, past events, and open source media, GAC determined that the information contributed to the exercise of the Royal Canadian Mounted Police (RCMP)'s and CSIS's jurisdiction, or the carrying out of their responsibilities, in respect of activities that undermine the security of Canada.

41. GAC disclosed the entirety of the information to both the RCMP and CSIS. The only information redacted was the name and contact information of the individual who provided the information to GAC.

42. GAC explained to NSIRA that it concluded that paragraph 5(1)(b) of the SCIDA was met because it did not identify a reasonable expectation of privacy in the content of the private social media group. NSIRA observes that GAC did not consider all of the relevant factors that would allow it to satisfy itself that the disclosure would not affect any person's privacy interest more than is reasonably necessary in the circumstances. As such, the disclosure of information did not meet the second threshold requirement under subsection 5(1) of the SCIDA. Therefore, the

disclosure of personal information of the group members did not comply with the requirements of the SCIDA.

Finding no. 4: NSIRA finds that, in ten out of thirteen disclosures, GAC satisfied itself that the disclosure will not affect any person's privacy interest more than reasonably necessary in the circumstances, as required under paragraph 5(1)(b) of the SCIDA.

Accuracy and Reliability Statements

43. The Arar Report noted that "sharing unreliable or inaccurate information does not provide a sound foundation for identifying and thwarting real and dangerous threats to national security and can cause irreparable harm to individuals."[18]

44. A core theme in the SCIDA's guiding principles is that of effective and responsible disclosure of information. Disclosing institutions are required, under subsection 5(2) of SCIDA, to provide information at the time of disclosure regarding the accuracy of the information disclosed and the reliability of the manner in which it was obtained.

45. Given the valuable context that accuracy and reliability statements provide to disclosures, precise and complete statements tailored to the specific circumstances of the disclosure can help avoid false perceptions, and can help ensure that recipient institutions have a clear understanding as to the accuracy and reliability of the information disclosed.

46. GAC relied on the PS Guide as its primary policy guidance document on the SCIDA. The PS Guide sets out that ensuring that the information disclosed is as accurate, complete, and as up-to-date as possible is key to responsible and effective information sharing.[19]

47. GAC informed NSIRA that partner agencies can better verify the accuracy of the information and the reliability of its source than GAC. NSIRA agrees that in some instances, GAC has limited capability for verification. Nonetheless, the SCIDA requires accuracy and reliability

[18] Arar Report (Analysis and Recommendations), p. 335.

[19] PS Guide, p. 19.

statements in every disclosure; accuracy and reliability statements must be clear and context-specific in order to be meaningful.

48. In an example of a well-developed statement, GAC provided the following:

> The information disclosed by GAC was obtained through interactions between GAC officials with [known and credible source X and another individual]. GAC is not in a position to assess the accuracy and reliability of the above information provided to GAC officials by [these individuals]. GAC assesses that [source X] is highly credible, and is likely providing reliable information.

In this case, the statement made a distinction between the accuracy and reliability of the information disclosed, depending on the source of that information. The disclosure sets out which information was provided by which source.

49. Overall, eleven of the thirteen disclosures contained accuracy and reliability statements. Two disclosures did not include the statement as the SCIDA requires. These omissions were not tied to GAC's inability to verify the accuracy and reliability of the information.

Finding no. 5: NSIRA finds that two out of thirteen disclosures did not contain accuracy and reliability statements as required by subsection 5(2) of the SCIDA.

Recommendation no. 2: NSIRA recommends that in order to provide the most valuable and meaningful context for the recipient institution, accuracy and reliability statements should be clear and specific to the circumstances of the disclosure.

Record-keeping

50. Paragraph 9(1)(e) of the SCIDA requires that disclosing institutions prepare a description of the information that they relied on to satisfy themselves that the disclosure was authorized under the SCIDA, including that the disclosure did not affect privacy interests more than reasonably necessary, as part of their record-keeping obligations under the SCIDA.

51. It is noted that the PS Guide sets out the steps to making a disclosure, which include creating a record describing the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under the SCIDA. Furthermore, the PS Guide's Appendix A: Record-keeping Template for Institutions Disclosing Information under the SCIDA, which is intended to help departments meet record-keeping obligations for disclosing institutions under the SCIDA, contains a field for departments to describe that information. It also restates the requirements under paragraphs 5(1)(a) and (b) of the SCIDA that the disclosing institution be satisfied that the disclosure will contribute to the recipient institution's national security mandate, and will not affect any person's privacy interest more than reasonably necessary in the circumstances.

52. The SCIDA 2020 Review observed that GAC's records describing the information it used to satisfy itself that certain responsive disclosures to CSIS, were robust. The basis for this observation was that GAC's records contained information provided by CSIS to aid in GAC's assessment, including details of the potential impact on the subject(s) of the request.[20]

53. During the course of this year's review, NSIRA requested that GAC provide a description of how it satisfied itself that the disclosure was authorized under both threshold requirements under the SCIDA. NSIRA also requested that GAC provide all supporting documents GAC relied on in its assessment. GAC provided explanations in response to NSIRA's queries in this regard, referencing supporting documents. Based on a review of the records provided, NSIRA observes that GAC's practices could be improved by contemporaneously and expressly articulating which information it relied on to satisfy itself that the disclosures would not impact any person's privacy interest more than reasonably necessary in the circumstances.

Recommendation no. 3: NSIRA recommends that all disclosing departments contemporaneously prepare descriptions of the information that was relied on to satisfy themselves that disclosures were authorized under the SCIDA.

Training on the SCIDA

54. GAC used four distinct PowerPoint documents in 2021 to train employees on the SCIDA.

[20] SCIDA 2020 Review, p. 30.

55. A course entitled Governance, Access, Espionage and Technical Security (GATE) was accessible to all employees going on postings as an introductory course focused on the awareness of information security at GAC. This presentation did not include practical examples or scenarios, but explained that any information sharing under the SCIDA must be done through GAC Headquarters.

56. Furthermore, a presentation provided by the Director General of the Intelligence Bureau to the majority of Heads of Mission going on postings, as an introductory course on intelligence support and security, did not provide illustrative examples or scenarios, but set out that information sharing under the SCIDA must be done through Headquarters.

57. Finally, the Department of Justice legal team provided two presentations: one to Global Security Reporting Program Officers going on postings as an introduction to information sharing policies and practices, including several slides on the SCIDA, and the other to groups of employees at Headquarters as an introduction to information sharing policies and practices. NSIRA noted that each presentation included only one or two examples illustrating the considerations in making a disclosure under the SCIDA.

58. Three of the four presentations also included a range of information about record-keeping requirements. However, the information in the presentations was largely limited to reiterating the requirements under the SCIDA, and no practical examples or scenarios were provided. Similarly, while these presentations reiterated requirements under the SCIDA to include accuracy and reliability statements, no practical examples were provided.

Finding no. 6: NSIRA finds that GAC training on the SCIDA lacks sufficient illustrative examples required to provide employees with adequate guidance to fulfill their obligations under the SCIDA.

Recommendation no. 4: NSIRA recommends that additional illustrative examples and scenarios be included in the SCIDA training, including for disclosure threshold requirements, accuracy and reliability statements and record-keeping requirements.

4. RESPONSIVENESS AND PROVISION OF INFORMATION

59. All departments met the timelines for the provision of information to NSIRA.

60. Subsections 9(1) and 9(2) of the SCIDA contain record-keeping obligations for disclosing and recipient institutions. Subsection 9(3) of the SCIDA requires all departments to provide every record prepared under those subsections to NSIRA, for the purpose of NSIRA's annual review of disclosures under SCIDA. Not only is thorough record-keeping a legal requirement for disclosing and recipient institutions, it is not possible for NSIRA to fulfill its mandated annual review without all records from all departments.

61. This review focussed on GAC proactive disclosures. NSIRA conducted a cross-comparison of the number of disclosures reported by GAC and those received by recipient institutions and notes that the numbers align. NSIRA did not independently verify the completeness of the records provided by GAC. Nonetheless, the assessment under the SCIDA requires GAC to demonstrate compliance. Additional requests for information over the course of the review led NSIRA to conclude that it received all information necessary to conduct the review. Finally, GAC had the opportunity to review a preliminary draft of this report and provide additional information. For these reasons, NSIRA is confident that it received all information necessary to conduct the review.

5. CONCLUSION

62. The SCIDA is a legislative tool meant to encourage and facilitate the responsible and effective disclosure of national security-related information between federal government institutions. Of the thirteen disclosures in the review sample, three did not meet one or both disclosure threshold requirements and two did not contain accuracy and reliability statements. Prior to consulting on potential disclosures, departments should consider what information is necessary to include in the consultation. Departments should also contemporaneously document on what basis they were satisfied that disclosures were authorized under the SCIDA. Furthermore, improvements to ongoing training are recommended, to provide more illustrative examples to guide employees in fulfilling their obligations under the SCIDA. NSIRA looks forward to revisiting the implementation of the SCIDA in future years and expects to find improved compliance, record-keeping, and delivery of training programs.

ANNEX A. SCIDA BACKGROUND

1. The perceived need for stand-alone legislation to govern information disclosure between federal departments for national security purposes was borne largely out of gaps identified by prior independent commissions charged with reviewing specific national security incidents. The SCIDA represents part of the Government of Canada's response to calls for reform from the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (Air India Inquiry), and the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (Arar Inquiry), among others.[21] These reviews highlighted the serious and tragic consequences that can result when federal departments fail to share national security information in a timely, coordinated, or responsible manner.

2. A brief summary of the context and ultimate findings of these Inquiries with respect to national security information is useful in understanding the underlying rationale for the SCIDA.

Air India Inquiry

3. The Air India Inquiry reviewed the events that led to the 1985 terrorist bombing of an Air India aircraft while in flight. In conducting its review, the Inquiry considered the actions and interactions of a number of federal institutions, including the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), the Department of External Affairs, the Communications Security Establishment, and Transport Canada. It found that the failure of these domestic agencies to share timely and critical information resulted in numerous missed opportunities to properly assess and address the threat.[22]

---

[21] Canada, Air India Review Secretariat, *Lessons to be Learned: The report of the Honourable Bob Rae, Independent Advisor to the Minister of Public Safety and Emergency Preparedness, on outstanding questions with respect to the bombing of Air India Flight 182*, by Bob Rae, (Ottawa: Air India Review Secretariat, 2005) at 23. See Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar – Analysis and Recommendations*, (Ottawa: Public Works and Government Services Canada, 2006) at 331. Public Safety Canada also reports that the need for legislation responded, in part, to the findings of Status Reports of the Auditor General of Canada (2004 and 2009) and the Reports of the Standing Committee on Public Accounts concerning those Auditor General reports (2005 and 2009). See *Security of Canada Information Disclosure Act – A Step-by-Step Guide to Responsible Information Sharing* (December 2019).

[22] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy: Final Report*, vol 2, Part 1: Pre-Bombing (Public Works and Government Services Canada, 2010) s 3.5 Information-Sharing Failures at 390-427, s 3.6 Lack of Government-Wide Coordination in the Threat Assessment Process at 437, and s 4.4 Failures in Sharing of Information at 491-508.

4. The Inquiry cited a number of factors that contributed to flawed inter-agency communication, including the siloed intelligence system, gaps in training, failures in the internal handling and communication of information, a poor understanding of the mandates and jurisdictions of other federal organizations, a lack of consistent criteria to guide when information should be shared, insufficient interdepartmental dialogue, informal and *ad hoc* modes of inter-departmental communication, a failure to recognize the importance of other agencies' information, and a lack of government-wide coordination in threat assessment.[23] Indeed, at the time, although some in the federal government had recognized the need to create a centralized and consistent system to improve information sharing, no action was taken.[24]

5. The Inquiry concluded that the failure of domestic agencies to share information in an effective manner contributed to the downing of the Air India flight, killing all 329 on board, mostly Canadians. Until the September 11 attacks in the United States, the bombing of Air India Flight 182 remained the world's deadliest incident of air terrorism. It is the worst-ever terrorist attack in Canadian history.[25]

Arar Inquiry

6. The Arar Inquiry investigated the 2002 detention of Canadian citizen Maher Arar in the United States, his subsequent deportation to Syria, and his nearly year-long imprisonment and mistreatment in Syria, where he was interrogated, tortured, and held in degrading and inhumane circumstances. Mr. Arar had come to the RCMP's attention in a terrorism investigation in which the RCMP had identified him as a person of interest, but not a suspect or a target of that

[23] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy: Final Report*, vol 2, Part 1: Pre-Bombing (Public Works and Government Services Canada, 2010) (Air India Inquiry (Final Report)) s 3.5 Information-Sharing Failures at 390, 409, s 3.6 Lack of Government-Wide Coordination in the Threat Assessment Process at 427, 431, 433, and s 4.4 Failures in Sharing of Information at 491, 508.

[24] Air India Inquiry (Final Report) s. 4.4 Failures in Sharing of Information at 491.

[25] *The Government of Canada Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182*, (Action Plan), (Ottawa: Public Safety Canada, 2010) (Response to Air India Inquiry) at 1.

investigation.[26] In fact, the Inquiry concluded that there was nothing to suggest that Mr. Arar had committed any offence or that his activities constituted a threat to the security of Canada.[27]

7. The Inquiry found that, when making the decisions to detain and remove Mr. Arar, American authorities very likely relied on the flawed information that the RCMP had provided.[28] The Inquiry found that the information shared by the RCMP failed to comply with its own internal policies that required screening for relevance, reliability, and personal information. The Inquiry also found that the information the RCMP shared was inaccurate, portrayed Mr. Arar in an unfairly negative fashion, and overstated his importance in its investigation. Further, the RCMP shared the information without attaching written caveats, again, as required by RCMP policy, which thereby increased the risk that the information would be used for unapproved purposes.

8. The Inquiry made recommendations to address its concerns with information sharing practices in RCMP national security investigations – however, it did not limit its recommendations to the RCMP's information sharing with foreign agencies. Rather, it extended the application of its recommendations to information sharing with domestic agencies as well. The Inquiry also did not limit these recommendations to the RCMP. It recommended their general application to other Canadian agencies that also engage in sharing information related to national security.

9. In its recommendations, the Inquiry acknowledged the importance of information sharing between domestic agencies for national security purposes. However, it stressed the need for information to be shared in a reliable and responsible fashion, including with the appropriate controls. It recommended that information only be shared for national security reasons once screened in accordance with certain principles – in particular, those of relevance, reliability, and accuracy – and in keeping with laws respecting personal information and human rights. It also

---

[26] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar – Factual Background*, vol 1 (Ottawa: Public Works and Government Services Canada, 2006), p. 53. The Inquiry defined the term "person of interest" as "someone whose role is not clear to the investigation team and about whom more information is required. The Inquiry described a "target" as "someone about whom the investigation team is trying to uncover evidence to support criminal charges". See also Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar – Analysis and Recommendations*, (Ottawa: Public Works and Government Services Canada, 2006) (Arar Report (Analysis and Recommendations)), p. 9.

[27] Arar Report (Analysis and Recommendations), p. 9.

[28] Arar Report (Analysis and Recommendations), p. 14.

stressed that information should never be shared without clear and precise written caveats setting out the restrictions on its use and further distribution.[29]

10. The Inquiry stressed that controls placed on shared information are meant to facilitate and promote the orderly flow of information, not to impede or stop it.[30] In screening for relevance, the Inquiry emphasized the need for those sharing the information to be satisfied that the information has some connection to the recipient institution's investigation and to the use to which the information will be put.[31] The Inquiry stated that the threshold for relevance need not be high, so long as the information is also appropriately screened for reliability, accuracy, privacy, and human rights, and includes the proper caveats.[32]

11. The Inquiry underscored the importance of screening for reliability and accuracy, stating that:

> Sharing unreliable or inaccurate information does not provide a sound foundation for identifying and thwarting real and dangerous threats to national security and can cause irreparable harm to individuals.[33]

12. The Inquiry noted that the concept of reliability relates primarily to the source of the information. It stated that all agencies involved in information sharing must be vigilant about accuracy, and about precision when describing facts or events, or when information contains an assessment or evaluation of an individual or an individual's status in an investigation. It indicated approval for the RCMP's system of grading sources and information as 'reliable', 'believed reliable', 'of unknown reliability' or 'of doubtful reliability'. The highest category of reliability would only be assigned if every effort had been made to validate the information, coupled with "a combination of proven accuracy of information and proven dependability as a person".[34] The lowest category would apply where there is doubt about the source or the information.[35]

---

[29] Arar Report (Analysis and Recommendations), pp. 366-367, Recommendations 6-11.

[30] Arar Report (Analysis and Recommendations), p. 331.

[31] The Inquiry also noted that relevance, in some instances, may include information to be provided to another agency to seek assistance from that agency in an investigation, in this case, an RCMP investigation. See Arar Report (Analysis and Recommendations), p. 335.

[32] Arar Report (Analysis and Recommendations), p. 335.

[33] Arar Report (Analysis and Recommendations), p. 335.

[34] Arar Report (Analysis and Recommendations), pp. 335-336.

[35] Arar Report (Analysis and Recommendations), p. 336.

Government Response: The SCISA

13. In 2010, the Government of Canada published its official response to the Air India Inquiry. Its *Action Plan* acknowledged the importance of comprehensive, seamless, and coordinated information sharing between federal departments and agencies charged with ensuring the safety and security of Canadians.[36] It also stated that where there are complex and numerous laws and policies that govern the use of personal information, these can hinder appropriate information sharing in this context.[37]

14. The Government's *Action Plan* sought to enhance interdepartmental cooperation and address barriers to information sharing, in part, by introducing new legislation to enable information to be shared for the purposes of national security.[38] The result was the *Security of Information Sharing Act* (SCISA),[39] which was enacted in 2015 as part of the *Anti-Terrorism Act, 2015* (former Bill C-51), and was the precursor to the SCIDA. The SCISA allowed federal institutions to disclose information if relevant to the recipient's jurisdiction or responsibilities in respect of "activities that undermine the security of Canada".

The SCIDA

15. In 2016, the Government held consultations with members of the public, stakeholders and subject matter experts on national security and the protection of rights and freedoms.[40] The SCISA was amended in 2019 through the *National Security Act, 2017* (former Bill C-59), and was renamed the *Security of Canada Information Disclosure Act* (SCIDA).[41]

---

[36] Response to Air India Inquiry, p. 7.

[37] Response to Air India Inquiry, p. 7.

[38] Response to Air India Inquiry, p. 7.

[39] *Security of Canada Information Sharing Act*, SC 2015, c 20, s 2, as repealed and re-enacted by *Security of Canada Information Disclosure Act*, SC 2015, c 20, s 2.

[40] "National Security Consultations: What We Learned Report" (19 May 2017) at 8, online (PDF): Public Safety Canada ,<www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-nsc-wwlr/index-en.aspx#a08>.

[41] SCIDA is the Act's short title. Its long title, as discussed below, is *An Act to encourage and facilitate the disclosure of information between Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada.*

16. The SCIDA allows Government of Canada institutions[42] to disclose information, including personal information, that is relevant to activities that undermine the security of Canada, to a select group of federal institutions with national security mandates. Disclosures are either made proactively, on the own initiative of a Government of Canada institution, or in response to a request by an institution authorized to receive information under the SCIDA.

17. The amendments that resulted in the SCIDA included: replacing the standard of "relevance" with the two-part standard requiring that the disclosing institution must be satisfied that the disclosure will contribute to the recipient's national security jurisdiction in respect of activities that undermine the security of Canada, and will not affect any person's privacy interest more than reasonably necessary; further clarifying the definition for "activity that undermines the security of Canada", and excluding from that definition the activities of advocacy, protest, dissent, and artistic expression; requiring statements of accuracy and reliability to accompany any information disclosure; and requiring federal institutions to prepare and keep records of any information disclosed or received, with a copy of such records to be provided to NSIRA for its annual review of disclosures under the Act.

18. The SCIDA's designated long title also reflects its stated purpose: *An Act to encourage and facilitate the disclosure of information between Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada*.[43]

19. The SCIDA lists a number of guiding principles, including:

- The effective and responsible disclosure of information;
- Respect for caveats on and originator control over disclosed information;
- Entry into information sharing arrangements where there is regular information disclosure to the same federal institution;
- The provision of feedback as to how disclosed information is used and whether it is useful in achieving the Act's purpose and facilitating effective and responsible information disclosure; and
- That only those within the recipient institution who exercise its jurisdiction or carry out its responsibilities in respect of activities that undermine the security of Canada ought to receive the information disclosed under the Act.

---

[42] The term "Government of Canada institution" is defined by linking to the definition of the same term in the *Privacy Act*, subject to any exclusions listed in Schedule 1 of the SCIDA. See SCIDA, ss. 2(1).

[43] See also *Security of Canada Information Disclosure Act*, SC 2015, c 20, s 2, s 3.

20. The SCIDA's core provision involves an expanded threshold for determining, prior to any disclosure, whether information in a federal institution's possession can be responsibly disclosed. Subsection 5(1) specifies that information can only be disclosed if the disclosing institution is satisfied that the disclosure:

- Will contribute to the exercise of the recipient institution's jurisdiction, or the carrying out of its responsibilities, under an Act of Parliament or another lawful authority, in respect of activities that undermine the security of Canada; and
- Will not affect any person's privacy interest more than is reasonably necessary under the circumstances.

21. The SCIDA also includes specific record-keeping obligations for each of the disclosing and recipient institutions. The SCIDA requires all disclosing institutions to prepare and keep records that include a description of the information disclosed, as well as a description of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under the SCIDA.

22. Finally, each federal institution's authority to collect, disclose, retain and use information, including personal information, remains circumscribed by law, including the *Canadian Charter of Rights and Freedoms* (Charter), and the *Privacy Act*. The SCIDA does not take precedence over any other statutory or regulatory prohibitions or limitations on the disclosure of information.[44]

[44] See *Security of Canada Information Disclosure Act – A Step-by-Step Guide to Responsible Information Sharing* (December 2019), p. 7.

ANNEX B. SCIDA BY THE NUMBERS

Total Disclosures under the SCIDA

1. As illustrated in the following table, Immigration, Refugees and Citizenship Canada (IRCC) made the highest number of disclosures under the SCIDA, with a total of 149 disclosures. Global Affairs Canada (GAC) made a total of 44 disclosures, and the Department of National Defence/Canadian Armed Forces (DND/CAF) made two disclosures. In total, 195 disclosures were made under the SCIDA in 2021.

Disclosing Institution	Receiving Institution	Number of Disclosures (proactive and responsive)
GAC	CSIS	41
GAC	RCMP	2
GAC	IRCC	1
IRCC	CSIS	79
IRCC	CSE	68
IRCC	GAC	2
DND/CAF	CSIS	2
	Total	195

Total Proactive Disclosures

2. GAC made the majority of proactive disclosures under the SCIDA. Thirteen out of a total of eighteen proactive disclosures were made by GAC, while two were made by DND/CAF and three were made by IRCC.

Disclosing Institution	Number of Proactive Disclosures
GAC	13
DND/CAF	2
IRCC	3
Total	18

Proactive Disclosures by GAC

3. Nearly all GAC proactive disclosures were made to the Canadian Security Intelligence Service (CSIS). Two other proactive disclosure were made to the Royal Canadian Mounted Police (RCMP).

Recipient Institution	Number of Proactive Disclosures
CSIS	11
RCMP	2

ANNEX C. SECURITY OF CANADA INFORMATION DISCLOSURE ACT (SCIDA) LEGAL FRAMEWORK

1. The purpose of the SCIDA is to encourage and facilitate the disclosure of information between federal institutions, to protect Canada against activities that undermine the country's security.[45] The SCIDA does not authorize the collection of information,[46] and only authorizes the disclosure of information to the following 17 recipient government institutions.

Federal institutions that can receive information under the SCIDA[47]

Canada Border Services Agency	Department of Foreign Affairs, Trade and Development (Global Affairs Canada)
Canada Revenue Agency	Department of Health
Canadian Armed Forces	Department of National Defence
Canadian Food Inspection Agency	Department of Public Safety and Emergency Preparedness (Public Safety Canada)
Canadian Nuclear Safety Commission	Department of Transport
Canadian Security Intelligence Service	Financial Transactions and Reports Analysis Centre of Canada

[45] *Security of Canada Information Disclosure Act*, SC 2015, c 20, s 2, s 3 (SCIDA), s. 3

[46] SCIDA, s. 6

[47] SCIDA, Schedule 3

Communications Security Establishment	Public Health Agency of Canada
Department of Citizenship and Immigration	Royal Canadian Mounted Police
Department of Finance	

1. Over one hundred federal institutions may, on their own initiative or upon request, disclose information to the 17 designated federal institutions, if the disclosing institution satisfies itself that the disclosure of information:

a) will contribute to the exercise of the recipient institution's jurisdiction, or the carrying out of its responsibilities, under an Act of Parliament or another lawful authority, in respect of activities that undermine the security of Canada,[48] and
b) will not affect any person's privacy interest more than is reasonably necessary.[49]

3. The SCIDA defines what is meant by "activity that undermines the security of Canada" as any activity that:

a) undermines the sovereignty, security or territorial integrity of Canada;
b) threatens the lives or the security of people in Canada; or
c) threatens the life or the security of any individual who has a connection to Canada and who is outside Canada.[50]

4. Several examples are included in the definition of an "activity that undermines the security of Canada," such as:

a) Espionage, sabotage or covert foreign-influenced activities;
b) Terrorism; and

[48] SCIDA, para. 5(1)(a)
[49] SCIDA, para. 5(1)(b)
[50] SCIDA, ss. 2(1)

c) Conduct that takes place in Canada that undermines the security of another state.[51]

5. However, The SCIDA sets out an exception to this definition. Advocacy, protest, dissent, or artistic expression, unless carried on in conjunction with an activity that undermines the security of Canada, do not constitute activities that undermines the security of Canada.[52]

6. The SCIDA also includes other requirements, notably that:

a) An institution that discloses information must, at the time of the disclosure, also provide information regarding its accuracy and the reliability of the manner in which it was obtained.[53]
b) An institution must destroy or return any personal information, received via a SCIDA disclosure, that is not necessary for the institution to exercise its jurisdiction, or to carry out its responsibilities, under lawful authority, in respect of activities that undermine the security of Canada.[54]
c) Every institution that discloses or receives information under the SCIDA must prepare and keep records setting out certain information, such as a description of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under the SCIDA. Furthermore, these records must be submitted to NSIRA within 30 days after the end of each calendar year.[55]

7. In addition, the SCIDA's guiding principles are as follows: (i) effective and responsible disclosure protects Canada and Canadians; (ii) respect for any caveats on disclosed information; (iii) entry into information-sharing arrangements where information is regularly disclosed; (iv) provision of feedback as to how disclosed information is used and whether it is useful; and (v) limits on who within an institution should receive information disclosed under the SCIDA.[56]

---

[51] SCIDA, ss. 2(1)

[52] SCIDA, ss. 2(2)

[53] SCIDA, ss. 5(2)

[54] SCIDA, s. 5.1. This requirement "does not apply to the Canadian Security Intelligence Service in respect of any information that relates to the performance of its duties and functions under section 12 of the Canadian Security Intelligence Service Act." SCIDA, ss. 5.1 (3)

[55] SCIDA, s. 9.

[56] SCIDA, s. 4

ANNEX D. FINDINGS AND RECOMMENDATIONS

Findings

1. NSIRA finds that, in twelve out of thirteen disclosures, GAC demonstrated that it satisfied itself as to the contribution of the information to the recipient institution's responsibilities in respect of activities that undermine the security of Canada, as required under paragraph 5(1)(a) of the SCIDA.

2. NSIRA finds that, without first conducting the analysis under paragraph 5(1)(a) of the SCIDA, departments risk disclosing information that does not pertain to the national security mandate of the recipient institution or to activities that undermine the security of Canada.

3. NSIRA finds that, in one of thirteen disclosures, GAC consulted on more information than necessary to obtain confirmation from CSIS that the disclosure contributed to its mandate and was linked to activities that undermine the security of Canada.

4. NSIRA finds that, in ten out of thirteen disclosures, GAC demonstrated that it satisfied itself that the disclosure will not affect any person's privacy interest more than reasonably necessary in the circumstances, as required under paragraph 5(1)(b) of the SCIDA.

5. NSIRA finds that two of thirteen disclosures did not contain accuracy and reliability statements as required by subsection 5(2) of the SCIDA.

6. NSIRA finds that GAC training on the SCIDA lacks sufficient illustrative examples required to provide employees with adequate guidance to fulfill their obligations under the SCIDA.

Recommendations

1. NSIRA recommends that consultations be limited to the information necessary to obtain confirmation from the potential recipient that the information contributes to its mandate and is linked to activities that undermine the security of Canada.

2. NSIRA recommends that in order to provide the most valuable and meaningful context for the recipient institution, accuracy and reliability statements should be clear and specific to the circumstances of the disclosure.

3. NSIRA recommends that all disclosing departments contemporaneously prepare descriptions of the information that was relied on to satisfy themselves that disclosures were authorized under the SCIDA.

4. NSIRA recommends that additional illustrative examples and scenarios be included in the SCIDA training, including for disclosure threshold requirements, accuracy and reliability statements and record-keeping requirements.