National Security and Intelligence Review Agency

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

NSIRA

NSIRA's 2019 Annual Report on the Disclosure of Information under the *Security of Canada Information Disclosure Act*

Canada's independent expert review body for all national security and intelligence activities

Canada

November 24, 2020

The Honourable Bill Blair, P.C., M.P.
Minister of Public Safety and
Emergency Preparedness
269 Laurier Avenue West
Ottawa, ON K1A 0P8

Dear Minister,

On behalf of the National Security and Intelligence Review Agency, it is my pleasure to present you with our first Annual Report of the *Security of Canada Information Disclosure Act* (SCIDA). As articulated in section 39 (1) of the *National Security and Intelligence Review Agency Act* (the "Act"), our report contains information with respect to the disclosures of information made under SCIDA during the previous calendar year. This review of SCIDA disclosures also took place under section 8(1)(b) of the Act, which allows NSIRA to review any activity carried out by a department that relates to national security.

In accordance with paragraph 52(1)(b) of the Act, our report was prepared after consultation with the deputy heads concerned in an effort to ensure that it does not contain information whose disclosure would be injurious to national security, national defence or international relations or that is subject to solicitor-client privilege or the professional secrecy of advocates and notaries or to litigation privilege.

Yours sincerely,

The Honourable Dr. Ian Holloway, P.C., C.D., Q.C.
Acting Chair
National Security and Intelligence Review Agency

Table of Contents

Abstract

Parliament enacted the *Security of Canada Information Disclosure Act* (SCIDA) in 2019 to improve the sharing of intelligence and national security information. SCIDA provisions aim to enhance accountability by clarifying roles and responsibilities in the disclosure process and amending the specific authority under which federal institutions may disclose this information. The National Security and Intelligence Review Agency (NSIRA) is responsible for reviewing and reporting annually on these disclosures. SCIDA has been used 114 times to disclose information during the reporting period of June 21 to December 31, 2019. The initial impression is that departments and agencies are making good progress to institutionalize this new legislative authority. The Royal Canadian Mounted Police and the Canadian Security Intelligence Service were the main recipients of SCIDA disclosures; Immigration, Refugees and Citizenship Canada and Global Affairs Canada were the main disclosers of information. The content of these disclosures varied, but generally involved personal information: names, age, physical characteristics, location and residential information. Departments and agencies varied significantly in how they applied certain SCIDA requirements. For example, the level of detail varied in statements disclosing institutions made to recipients concerning the accuracy, reliability and origin of information. In determining whether to disclose information, departments and agencies were also inconsistent in how they applied the contribution test, that is, determining whether disclosure would contribute to the exercise of the recipient's jurisdiction, or the carrying out of its responsibilities in respect of activities that undermine the security of Canada. In addition, NSIRA identified some requests for information that were broad in nature, raising a risk that extraneous personal information could have been inadvertently shared. Finally, NSIRA observed two instances of departments or agencies destroying or returning information that either exceeded initial requests or was not necessary for the institution to exercise its jurisdiction. NSIRA also observed that the disclosures contained caveats.

Executive Summary

1. The *Security of Canada Information Disclosure Act* (SCIDA) promotes the disclosure of certain information between institutions of the Government of Canada in order to protect Canada against activities that undermine the nation's security. SCIDA is an updated statute intended to improve the sharing of intelligence and national security information, as well as to enhance accountability by clarifying roles and responsibilities in the disclosure process and amending the specific authority under which federal institutions may disclose this information.

2. Our agency, the National Security and Intelligence Review Agency (NSIRA), is required under its governing legislation to submit an annual report to the Minister of Public Safety and Emergency Preparedness on disclosures made under SCIDA. We have prepared this report to fulfil that obligation. This report is also intended to provide an overview of SCIDA and the obligations that it has created for federal departments and agencies.

3. Because SCIDA came into force only in June 2019, this report is based on a period of just six months; going forward, the reporting period will be a full calendar year. In addition, given the unprecedented nature of the COVID-19 pandemic, and its impact on our work, we could not complete our review of the disclosures made under SCIDA in 2019 in time for this publication. We are continuing our analysis of the disclosures, however, and intend to publish our findings in next year's report.

4. In the last six months of 2019, departments and agencies made 114 disclosures under SCIDA. Immigration, Refugees and Citizenship Canada made almost half of these disclosures, primarily to the Canadian Security Intelligence Service and the Royal Canadian Mounted Police. The content of these disclosures varied, but was generally concerned with personal information: names, age, physical characteristics, location and residential information.

5. Public Safety Canada has primary responsibility for coordinating the implementation of SCIDA. While we will return to this theme next year, our initial impression is that good progress is being made to institutionalize this new legislative authority.

6. Finally, we are also pleased to report that we have laid a foundation for working collaboratively with the Office of the Privacy Commissioner of Canada (OPC) on next year's annual review of SCIDA. The *National Security and Intelligence Review Agency Act* specifically allows for us to coordinate with the OPC; this will enable us to undertake a more comprehensive analysis of disclosures of information under SCIDA. Our goal is to produce a joint NSIRA-OPC report on SCIDA disclosures in 2021.

Background

7. Sharing information in a timely and effective manner is critical to assessing and mitigating threats, which can be complex and global in scope, and often evolve rapidly. Generally, departments and agencies share information with one another under the authority of, and consistent with, legal frameworks specific to their mandates. Disclosures must also be compliant with the *Privacy Act.* That legislation sets out that, except in specific limited circumstances, personal information under the control of a government institution shall not be disclosed without the consent of the individual. One exception is that information may be shared without consent when the purpose for disclosure is consistent with the original purpose for which the information was obtained or compiled. This exception, under section 8 of the *Privacy Act,* is known as "consistent use."

8. Problems with respect to information sharing date back to at least the 1980s. They were apparent in the work of Justice Major's Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182,[1] which addressed information sharing in relation to the bombing. The 2010 inquiry concluded that the failure of domestic agencies to share information effectively contributed to the downing of the Air India flight, and that information sharing lacked coordination, was unstructured and was inconsistent.[2]

9. In 2010, the government released its "Action Plan – The Government of Canada Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182."[3] This action plan led to the *Security of Canada Information Sharing Act* (SCISA), which came into force in 2015. SCISA's goal was to facilitate information sharing for national security purposes. In 2019, the legislation was amended and renamed the *Security of Canada Information Disclosure Act* (SCIDA) in response to concerns expressed by various stakeholders and the general public.[4]

10. SCIDA provides an independent authority for federal government institutions to disclose information to protect against activities that undermine the security of Canada. It is meant to improve the effectiveness and accountability of national security and intelligence information sharing by clarifying roles and responsibilities in the disclosure process, and by amending the specific legislative authority under which federal institutions are able to disclose this information.

11. Information sharing that takes place under SCIDA remains a small fraction of the information that is shared for national security purposes. Most information sharing continues to take place under the authority of the specific legal frameworks of the relevant departments, and under the authority of the *Privacy Act*, particularly its consistent use provision.

This Report

12. The National Security and Intelligence Review Agency (NSIRA) is required under its governing legislation[5] to submit to the Minister of Public Safety and Emergency Preparedness a yearly report on disclosures made under SCIDA. This report fulfils NSIRA's statutory obligation and is an essential component of the accountability measures in SCIDA. This report and NSIRA's annual public report are important vehicles through which NSIRA hopes to contribute to transparency with respect to the national security and intelligence activities of federal departments and agencies.

13. Given the unprecedented circumstances created by the COVID-19 pandemic and how it has affected NSIRA's work, the agency regrets that it was unable to complete in time for publication its assessment of the extent to which the 2019 SCIDA disclosures were legally compliant, as well as the extent to which these disclosures were reasonable and necessary. NSIRA is continuing to analyze these disclosures, however, and intends to publish its findings in next year's SCIDA report. Instead, this year's SCIDA report will provide parliamentarians and Canadians with information about SCIDA and how it fits alongside other legal mechanisms for the sharing of information, as well as provide baseline information on the disclosures for this reporting period. It also sets out NSIRA's expectations and intentions for the future, and explains why information sharing is a critical issue for NSIRA.

14. In this regard, NSIRA is pleased to report that it has taken important steps to lay the foundation for working jointly with the Office of the Privacy Commissioner of Canada (OPC) on next year's annual review of SCIDA. Coordinating with the OPC, pursuant to both the *National Security and Intelligence Review Agency Act* and the *Privacy Act,* will allow for a more comprehensive report in respect of disclosures of information under SCIDA[6]. In addition to avoiding duplication, working collaboratively will ensure that NSIRA's expertise in national security is complemented by the OPC's privacy expertise, whose mandate is to oversee compliance with the *Privacy Act*. The goal is to produce a joint NSIRA-OPC report on SCIDA disclosures in 2021.

Initial Concerns with SCIDA's Predecessor, the *Security of Canada Information Sharing Act* (SCISA)

15. As noted, SCIDA was shaped by the government's consultations on national security matters in 2016,[7] as well as by Parliament's scrutiny of the bill. These efforts highlighted concerns among stakeholders and the general public that the legislation would permit too much sharing of personal information, and without appropriate mechanisms for accountability. Many commentators urged the government to enhance the legal threshold for disclosing information; they argued that the term "relevance" was too low. Several stakeholders also urged that the receipt of information be governed by a standard of necessity and proportionality and that a precise definition of "threats to the security of Canada," one modelled on the *Canadian Security Intelligence Service Act* (CSIS Act), be incorporated into the bill.

16. In 2017, the review body for CSIS at the time, the Security Intelligence Review Committee (SIRC), published a review of SCISA to examine how it affected information sharing between CSIS and its domestic partners.[8] That same year, the OPC published a report on SCISA intended to determine, among other things, whether departments and agencies had engaged in appropriate risk management activities to identify and minimize the privacy impacts of sharing.[9] Both SIRC and the OPC noted general deficiencies in tracking and record keeping; they expressed concerns about SCISA's lack of clear requirements in that regard, which were thought to be key to maintaining strict controls over information sharing.

17. In response to these concerns, the preamble in the proposed Act was amended to include a statement that disclosure of information must respect the *Privacy Act* and other privacy legislation, as well as the *Canadian Charter of Rights and Freedoms* (the Charter). Other legislative amendments to SCISA included a change to the previous threshold of relevance, and a new requirement that both the disclosing agency and the receiving agency perform assessments throughout the disclosure process. In addition, the legislation now contains retention, reporting and record-keeping requirements. NSIRA's analysis of the 2019 disclosures — still under way — focuses on these concerns in assessing whether the disclosures met all statutory obligations.

Legal Framework for Information Sharing

18. The SCIDA preamble now declares that one of the Act's objectives is to create an explicit authority to facilitate the effective and responsible disclosure of information to protect the security of Canada. SCIDA also stipulates that it cannot authorize a disclosure prohibited under another federal statute. It further stipulates that SCIDA does not constitute a lawful authority for a department or agency to collect information.

19. Under SCIDA, a disclosing department or agency must verify that the recipient is one of the 17 departments and agencies listed in schedule 3 authorized to receive disclosures.[10] It must also be satisfied that the disclosure will "contribute to the exercise of the recipient's jurisdiction, or the carrying out of its responsibilities in respect of activities that undermine the security of Canada" (paragraph 5(1)(a)). Importantly, information relating to lawful advocacy, protest, dissent and artistic expression cannot be disclosed unless conducted in conjunction with an activity that undermines the security of Canada. The disclosure must not "affect any person's privacy interest more than is reasonably necessary in the circumstances" (paragraph 5(1)(b)). Additionally, the disclosing department or agency "must provide information regarding its accuracy and the reliability of the manner in which it was obtained" (subsection 5(2)).

20. At the same time, the receiving department or agency is subject to specific requirements under the Act. In particular, it must assess the "personal information"[11] received in order to ensure that all information that is not necessary for the department or agency to exercise its jurisdiction, or to carry out its responsibilities in respect of activities that undermine the security of Canada, is promptly destroyed or returned. An exception to this requirement is if retention is otherwise required by law. For example, the requirement to destroy or return personal information does not apply to certain law enforcement bodies, including the RCMP, if they are subject to criminal law disclosure obligations.[12] Additionally, pursuant to subsection 5.1(3), the requirement to return or destroy personal information obtained pursuant to SCIDA does not apply to CSIS in respect of any information that relates to the performance of its duties and functions under section 12 of the CSIS Act to collect information and intelligence on threats to the security of Canada.

SCIDA INFORMATION SHARING SCHEME

BEFORE DISCLOSURE

GC institution requests information from another GC institution. The recipient institution must be listed in schedule 3 of the Act.

GC institution, on its own initiative, decides to disclose to a GC institution listed in schedule 3 of the Act.

The information that the GC institution is expected to share is in respect of activities that undermine the security of Canada as defined in s.2 of the Act.

DISCLOSURE TEST

The disclosing institution must be satisfied that:

a) 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; and

b) the disclosure will not affect any person's privacy interest more than it is reasonably necessary in the circumstances.

(paragraphs 5(1)(a) and 5(1)(b)).

OTHER REQUIREMENTS

Copy to NSIRA
In relation to the record keeping requirement, a copy of every record of disclosure shared or received must be provided every year to NSIRA. (subsec. 9(3))

Destroy or return
The receiver must, as soon as feasible after receiving disclosure, destroy or return any personal information that is not necessary for the institution to exercise its jurisdiction, or to carry out its responsibilities, under an Act of Parliament or another lawful authority, in respect of activities that undermine the security of Canada. (subsec. 5.1 (1))

(continued)

Accuracy and reliability
GC institution that discloses information under subsection (1) must, at the time of the disclosure, also provide information regarding its accuracy and the reliability of the manner in which it was obtained. (subsec. 5(2))

Recordkeeping
GC institution must, as soon as feasible after receiving it under section 5, destroy or return any personal information, as defined in section 3 of the *Privacy Act*, that is not necessary for the institution to exercise its jurisdiction, or to carry out its responsibilities, under an Act of Parliament or another lawful authority, in respect of activities that undermine the security of Canada (subsec. 5.1(1)) unless otherwise required by law. (subsec. 5.1(2))

CSIS - Exception
Recordkeeping requirement does not apply to CSIS in respect of any information that relates to the performance of its duties and functions under s. 12 of the CSIS Act.(subsec. 5.1(3))

SCIDA in Context

21. Currently, the information sharing that takes place under SCIDA represents a small fraction of the information that is shared for national security purposes among federal government departments and agencies. All sharing of personal information by the federal government must be done in conformity with the Charter. Of note, section 8 of the Charter protects against "unreasonable search or seizure" and applies wherever a person might have a reasonable expectation of privacy. An authority to share information does not guarantee that the sharing meets the standards derived from section 8 of the Charter, and this issue must be assessed on a case-by-case basis. The *Privacy Act* governs all handling of personal information by federal government departments and agencies. SCIDA, however, is specific, and relates to the disclosure of national security information. Both Acts work hand-in-glove.

22. Additionally, there are specific statutes under which information sharing may occur. For example, subsection 19(2) of the CSIS Act authorizes the disclosure of information obtained by CSIS, and sections 43, 44 and 46 of the *Communications Security Establishment Act* (CSE Act) authorize the disclosure of information obtained by the Communications Security Establishment (CSE), with both pieces of legislation specifying that the information had to be obtained in the performance of each agency's own duties in certain circumstances. Other examples of specific statutes permitting such information sharing include the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act,* the *Immigration and Refugee Protection Act* (IRPA), the *Customs Act*, and the *Secure Air Travel Act.* In addition to these statutory authorities, section 8 of SCIDA provides that information can also be shared under the Crown prerogative or common law authorities. Much information sharing in the national security context, however, is done pursuant to the various exemptions of the *Privacy Act*. The RCMP, for example, may rely on the *Privacy Act* to disclose personal information in various contexts, including programs that coordinate the sharing of personal information, such as the Criminal Intelligence Service and the Canadian Police Information Centre, which are administered pursuant to the RCMP's law enforcement mandate.

Disclosures to NSIRA

23. Proper record keeping is a key aspect of accountability, as a failure to document and track disclosures and receipts of information undermines the review function, whether external or internal.

24. Under subsection 9(1) of SCIDA, records must be kept by departments and agencies that disclose and receive such information. The records must include, among other baseline information, the information that disclosing departments and agencies relied on to satisfy themselves that they had the authority to disclose the information. Recipient departments and agencies must indicate whether the information has been destroyed or returned. Under subsection 9(3) of SCIDA, a copy of those records must be provided to NSIRA within 30 days after the end of each calendar year.

Statutory Requirement to Report Disclosures to NSIRA

25. NSIRA received records from all agencies that disclosed or received information on a timely basis. However, some discrepancies were detected such that the number of disclosures of information reported did not, in a minority of cases, match the reported receipts of information. NSIRA asked for, and was provided, explanations for these discrepancies and is satisfied that the root causes can be attributed to the newness of the regime and that there was no attempt to obscure the fact of information having been disclosed or received. NSIRA is aware of the community's ongoing efforts to address this, led by Public Safety Canada. NSIRA expects that, next year, there will be fewer or no discrepancies in the numbers reported. NSIRA also requested and received access to the disclosures themselves, from all departments and agencies that either disclosed or received information. The necessity to provide complete copies of all disclosures and receipts, in addition to a "record" of each disclosure as set out in SCIDA, is required to allow NSIRA to fully assess whether the departments and agencies met their statutory obligations.

Frequency of Disclosures

26. During the last six months of 2019, departments and agencies reported having used SCIDA 114 times to disclose information. In comparison, during the first six months after its predecessor SCISA was enacted in 2015, departments and agencies reported using that legislation to disclose information 58 times.[13]

2019 SCIDA Disclosures

A total of **114 disclosures** were sent and received by Government of Canada departments in 2019. The below table identifies by whom and to whom disclosures were sent and received, and the volume of 2019 disclosures under the SCIDA.

Disclosing institution	Number of disclosures	Receiving institution
Canada Border Services Agency	**2**	Royal Canadian Mounted Police
Canada Border Services Agency	**1**	Canadian Security Intelligence Service
Global Affairs Canada	**23**	Canadian Security Intelligence Service
Global Affairs Canada	**3**	Immigration, Refugees and Citizenship Canada
Global Affairs Canada	**1**	Public Safety Canada
Global Affairs Canada	**15**	Royal Canadian Mounted Police
Immigration, Refugees and Citizenship Canada	**17**	Canadian Security Intelligence Service
Immigration, Refugees and Citizenship Canada	**5**	Communications Security Establishment
Immigration, Refugees and Citizenship Canada	**1**	Department of National Defence and Canadian Armed Forces
Immigration, Refugees and Citizenship Canada	**36**	Royal Canadian Mounted Police
Royal Canadian Mounted Police	**4**	Canada Revenue Agency
Royal Canadian Mounted Police	**1**	Financial Transactions and Reports Analysis Centre of Canada
Royal Canadian Mounted Police	**1**	Immigration, Refugees and Citizenship Canada
Royal Canadian Mounted Police	**3**	Global Affairs Canada
Transport Canada	**1**	Royal Canadian Mounted Police

27. Not surprisingly, the main recipients of SCIDA disclosures were the RCMP and CSIS, both of which have the authority under their respective mandates to collect and retain information in the conduct of investigations in the national security context. SCIDA, by contrast, does not constitute an authority to collect information.

28. Information disclosed under SCIDA may be disclosed either proactively or in response to a specific request. In many cases, the RCMP and CSIS requested of their government partners to obtain information of relevance to their active investigations. Information was then disclosed responsively under the authority of SCIDA.

29. Immigration, Refugees and Citizenship Canada (IRCC) was responsible for approximately half of the disclosures made under SCIDA in 2019. This, too, is not surprising, considering IRCC's mandate to collect personal information about Canadians, permanent residents and foreign nationals under the IRPA, the *Citizenship Act* and the Canadian Passport Order. In general, records gathered during the course of applications for immigration to Canada were often the subject of disclosure. IRCC also supplied information about the status of individuals in Canada. In NSIRA's view, a great deal of the information disclosed by IRCC would be considered "personal information" as defined in the *Privacy Act* and incorporated in the SCIDA.

30. Global Affairs Canada (GAC) was responsible for slightly over a third of all disclosures. The information was obtained in the course of providing consular assistance to Canadians, or through engagement with host-country authorities in regards to consular cases. In a majority of cases, GAC proactively disclosed the information at issue.

31. The content of disclosures varied, but was generally concerned with personal information: names, age, physical characteristics, location and residential information. As noted, some of the disclosures merely involved advising whether an individual had status in Canada. Other disclosures included familial and relationship information. A few disclosures contained personal information on individuals connected to an investigation.

Anonymized Scenario Examples of SCIDA Disclosures

1. **RCMP request for disclosure from IRCC**
   The RCMP initiated a criminal investigation of an individual who applied for citizenship with personal finances potentially linked to terrorist investments. The RCMP requested descriptors, biographical information, employment history and other known selectors from IRCC that would assist in this investigation.

2. **RCMP request for disclosure from IRCC**
   The RCMP initiated a criminal investigation of individuals believed to be facilitators of a terrorism organization. The RCMP sought identification information (e.g., full names, citizenship, marital status, photographs) for these individuals, in addition to contact and locational data, as well as marital status and known family members to assist in this investigation.

3. **CSE request for disclosure from IRCC**
   CSE's request for disclosure sought to confirm whether a given individual held Canadian citizenship or other status in Canada. This information assists CSE as it is prohibited from targeting Canadians. IRCC disclosed the information as requested, with caveats to protect the individual's privacy rights when communicating back to third parties.

4. **RCMP disclosure to the Canada Revenue Agency (CRA)**
   The RCMP discloses information related to registered charities and individuals linked to them, in certain cases. This includes confirming whether organizations or individuals are or have been the subject of an investigation. The CRA is responsible for protecting the integrity of Canada's registration system for charities. This information supports them in their efforts to detect and address risk as it relates to terrorist abuse of Canada's charitable sector.

32. A very small number of disclosures targeted more than a single individual. These appeared to represent an efficiency because the grounds for requesting or disclosing were the same. Nevertheless, NSIRA will be attentive to these types of disclosures in future reviews, given the potential risks associated with disclosures of this nature.

Other Observations

33. The disclosures contained caveats related to the use and disclosure of information; NSIRA observed no refusals of caveats by requesters. The degree to which disclosures included statements concerning the accuracy, reliability and origin of information, however, varied. Simply put, the level of detail varied from disclosure to disclosure. Given the O'Connor Commission's finding that inaccurate information related to Maher Arar was shared with foreign partners, this is an important observation. Next year's review will look for a consistently high standard across departments and agencies in this regard.

34. In addition, there were instances in which, based on the broad nature of the request, NSIRA assessed that extraneous personal information could have been inadvertently shared. Responsible use of SCIDA depends on departments and agencies demonstrating caution and attention to detail throughout the process to ensure that the disclosure will not affect anyone's privacy interest more than is reasonably necessary in the circumstances. This becomes a challenge when requests are not precise, or are expansive in scope. In this

context, it is worth noting that NSIRA observed two instances of departments or agencies destroying or returning information that either exceeded initial requests or was not necessary for the institution to exercise its jurisdiction. NSIRA will pay particular attention to this issue in future reviews.

35. Finally, SCIDA specifies that a disclosing department or agency must be satisfied that the disclosure will "contribute to the exercise of the recipient's jurisdiction, or the carrying out of its responsibilities, in respect of activities that undermine the security of Canada."[14] This is known as the "contribution test."

36. NSIRA noted some variation in the application of this test from disclosure to disclosure. Some departments and agencies applied it to each disclosure on a case-by-case basis. Others applied blanket or generic statements for several different requests. It is the responsibility of the disclosing department or agency to satisfy itself, among other things, that the information disclosed will contribute to the mandate of the recipient institution. Requests for information should provide a rationale that is sufficiently detailed and nuanced so that the disclosing department or agency would be able to be satisfied that the information would contribute to the mandate of the recipient department or agency. This will be an area that NSIRA will closely scrutinize in the future.

Systems and Training

37. Public Safety Canada has assumed a lead role in promoting interagency cooperation with respect to SCIDA. The department established the Strategic Coordination Centre on Information Sharing. This centre is dedicated to providing support to federal departments and agencies in operationalizing SCIDA, advancing governmental knowledge related to information sharing, and better educating the public on issues of national security information sharing. The department also formed a working group comprising SCIDA's schedule 3 departments and agencies.

38. In late 2019, Public Safety Canada produced a 92-page explanatory guide, "A Step-by-Step Guide to Responsible Information Sharing." This guide provides contextual information to promote better understanding of the purpose of SCIDA. It provides supporting material to assist with practical implementation of the Act in an effort to achieve consistency across departments and agencies in the disclosure process and in record keeping. For example, the guide outlines the required actions to be taken to disclose and receive information under SCIDA, and includes checklists and record-keeping and disclosure templates. It also clearly describes the mandates of all 17 departments and agencies listed in SCIDA as an aid to disclosing departments and agencies, since they must understand these mandates before disclosing information. Overall, the guide

demonstrates a serious effort to educate the government on SCIDA and to encourage its use. Departments and agencies using SCIDA are encouraged by NSIRA to make its use of the materials, including the templates, developed by Public Safety Canada.

39. Since July 2019, Public Safety Canada has also held SCIDA training and information sessions. Between July 2019 and February 2020, 14 sessions attracted some 245 participants. These sessions traced the history of SCIDA, provided guidance as to its use, and engaged participants with case scenarios. Participant feedback indicates these sessions were well-received. Due to the COVID-19 pandemic, training is now being held virtually.

40. All departments and agencies listed in SCIDA as potential recipients received the guidance materials from Public Safety Canada and all departments and agencies that actively disclosed material participated in the training. Training materials were also distributed to the members of the working group. These efforts promote consistency across government departments and agencies, which supports NSIRA's review responsibilities. Training for other departments and agencies that are more likely to receive information under SCIDA was scheduled for spring 2020, but was postponed because of the pandemic.

41. Public Safety Canada also encourages departments and agencies to develop their own internal guidance materials to communicate SCIDA requirements in the context of their specific information holdings, and with regard to their specific responsibilities for handling that information. Some departments and agencies have already developed internal guidance materials to further support the use of SCIDA as an authority to disclose information and to complement the materials provided by Public Safety Canada. For example, IRCC has developed guidance material to support the responsible implementation of SCIDA, as has CSE. In future reviews, NSIRA will examine how departments and agencies have supported and educated staff internally.

Conclusion: The Way Forward

42. Next year, NSIRA's review will respond to the two key concerns expressed during the public debate about this legislation, namely, that it would permit the disclosure of too much personal information, and that the information would be shared without appropriate mechanisms for accountability. Specifically, the report will feature a detailed examination of SCIDA disclosures to verify that the requirements and limitations of the Act are being respected when information is disclosed. As noted, this review will be coordinated with the OPC and will include, pursuant to the OPC's mandate, a review of government departments and agencies' compliance with the Privacy Act with respect to disclosures made under SCIDA.

43. In formulating an assessment, NSIRA will expect departments and agencies to have complied with the thresholds and requirements identified in SCIDA and the *Privacy Act*, as well as other applicable laws related to both disclosures and receipt of information. This will include an assessment of whether, for example:

- the disclosures contributed to the exercise of the recipient department or agency's jurisdiction, or the discharge of its responsibilities;
- the disclosure affects any person's privacy interest more than was reasonably necessary in the circumstances;
- any personal information that was not necessary for the department or agency to exercise its jurisdiction, or to carry out its responsibilities, was returned or destroyed; and
- statements on the accuracy and reliability of the information were provided.

NSIRA will be attentive to the limitation on disclosing information related to lawful advocacy, protest, dissent and artistic expression.

44. NSIRA will also expect the departments and agencies to continue to respect the record-keeping and reporting requirements of SCIDA; to have taken reasonable steps to put in place required policies, training or guidance, and procedures to ensure compliance with SCIDA; and, finally, that established policies and procedures have been followed in all cases. NSIRA's analysis will be informed and guided by the initial observations made in relation to the 2019 SCIDA disclosures, as described above.

Endnotes

1 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, Final Report, June 17, 2010.

2 See, for example, Vol. 2, Part 1, Pre-Bombing, Section 4.4, Failures in Sharing of Information, and Vol. 4, section 3.4, Use of Intelligence in Aviation Security.

3 Action Plan: The Government of Canada Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, December 2010.

4 For a full discussion of the differences between SCISA and SCIDA, see the backgrounder prepared by Public Safety Canada, Parliamentary Passage of Bill C-59: the National Security Act, 2017 – Fulfilling Commitments to Address Former Bill C-51: Overview of New Measures.

5 National Security and Intelligence Review Agency Act (NSIRA Act), SC 2019, c 13, ss 39(1).

6 Subsection 37(5) of the Privacy Act permits the Privacy Commissioner to coordinate the Commissioner's activities under subsection 37(1) with those of National Security and Intelligence Review Agency under any of paragraphs 8(1)(a) to (c) of the NSIRA Act to avoid any duplication of work. Under subsection 37(1) of the Privacy Act, the Privacy Commissioner may, at his or her discretion, carry out investigations related to personal information under the control of government institutions to ensure compliance with sections 4 to 8 of the Privacy Act, which would include reviewing whether disclosures made by government institutions pursuant to section 5 of SCIDA also satisfy paragraph 8(2)(b) of the Privacy Act.

7 Canada, Our Security, Our Rights: National Security Green Paper, Background document, 2016.

8 Security Intelligence Review Committee, SIRC Annual Report 2016-2017, Section 2: Reviews, "The Security of Canada Information Sharing Act."

9 Office of the Privacy Commissioner of Canada, Review of the Operationalization of the Security of Canada Information Sharing Act, 2017.

10 See Security of Canada Information Disclosure Act (SCIDA), section 3, which identifies disclosure of information "between Government of Canada institutions."

11 SCIDA defines "personal information" by referring to the same term in section 3 of the Privacy Act: "information about an identifiable individual that is recorded in any form," such as "any identifying number, symbol or other particular assigned to the individual."

12. SCIDA, section 5.1 (2).

13. House of Commons, Safeguarding Canada's National Security While Protecting Canadians' Privacy Rights: Review of the Security of Canada Information Sharing Act (SCISA), Chapter 4, "Use and Application of the Security of Canada Information Sharing Act to Date," House of Commons, May 2017.

14. SCIDA, section 5(1)(a).