

Government of Canada response to the recommendations of the NSIRA and OPC review of federal institutions' disclosures of information under the *Security of Canada Information Disclosure Act* in 2020

NSIRA Recommendation	Related Findings(s)	Government Response	Explanation
<p>1. In light of the restrictions under section 8 of the Privacy Act for all disclosures of personal information, NSIRA and the OPC recommend that institutions with national security expertise ensure that when they request personal information for national security-related purposes from other federal institutions, they make it clear that their requests, in and of themselves, do not constitute or confer authority for the other institution to disclose personal information.</p>	<p>1. The example above is illustrative that national security-related personal information can be disclosed in situations where institutions are not conscious of the requirements for lawful authority to do so.</p>	<p>Agree</p>	<p>Since requests for information do not, in and of themselves, authorize federal institutions to disclose personal information, several Government of Canada departments and agencies have already developed and implemented internal policies to set clear expectations, consistent guidelines and record-keeping practices for the disclosure of personal information for national security purposes in accordance with lawful authorities. Importantly, each federal institution is responsible for knowing and implementing its obligations, and each Deputy Head is responsible for ensuring that directives and resources are put in place to fulfil these obligations.</p> <p>Public Safety Canada will continue to work with partner departments and agencies to provide federal institutions with access to training, guidance and other useful resources on national security information sharing that help to explain what the requirements are for disclosing this type of information in a lawful manner. Public Safety Canada will also update its SCIDA Guide and related templates for requesting and disclosing information under the SCIDA to support federal institutions in</p>

NSIRA Recommendation	Related Findings(s)	Government Response	Explanation
			understanding their authorities for requesting and disclosing national security information.
<p>2. NSIRA and the OPC recommend that the RCMP finish updating its SCIDA policy to support compliance with the disclosure test in the Act, and provide guidance to its decision-makers empowered to make SCIDA disclosures on the analysis required to satisfy themselves that the disclosure test is met; and, ensure that these decisions are properly documented.</p>	<p>2. NSIRA and the OPC found that almost all (approximately 99%) of the disclosures of information made under the Act in 2020 satisfied the disclosure test under paragraph 5(1)(a) based on information reviewed.</p> <p>3. NSIRA and the OPC found that almost all (approximately 99%) of the disclosures of information made under the Act in 2020, appear not to affect any persons' privacy interest more than was reasonably necessary in the circumstances based on information reviewed. However, one non-compliant disclosure by the RCMP represents the vast majority of all confirmed personal information that was disclosed under SCIDA in 2020.</p>	Agree	<p>The RCMP has made significant progress towards completing its SCIDA policy modernization since April 2021. This updated SCIDA policy will provide an RCMP-specific complement to Public Safety's broader guidance to federal partners on SCIDA disclosures. The RCMP's updated policy tailors SCIDA guidance to a law enforcement environment and will serve to empower RCMP decision-makers to confidently share national security information in a compliant manner and aid in ensuring that decisions to disclose personal information are properly documented.</p>
<p>3. First, NSIRA and the OPC recommend that the RCMP provide fulsome and accurate information to DND-CAF about the non-compliant disclosure. Second, NSIRA and the OPC recommend that consistent with section 5.1 of SCIDA, DND-CAF assess the necessity of retaining the personal information received in light of this new information, our findings, associated DND-CAF directives and other applicable policies.</p>	<p>2. NSIRA and the OPC found that almost all (approximately 99%) of the disclosures of information made under the Act in 2020 satisfied the disclosure test under paragraph 5(1)(a) based on information reviewed.</p> <p>3. NSIRA and the OPC found that almost all (approximately 99%) of the disclosures of information made</p>	Partially Agree	<p>The RCMP does not agree that it failed to provide fulsome and accurate information to DND-CAF. The RCMP disclosed information that they were satisfied would contribute to the responsibility of the Department of National Defence and the Canadian Armed Forces to identify potential threats to military personnel and to provide strategic warning of emerging threats, in support of their counter-terrorism mandate. At the time of the disclosure, the RCMP were satisfied that the</p>

NSIRA Recommendation	Related Findings(s)	Government Response	Explanation
	under the Act in 2020, appear not to affect any persons' privacy interest more than was reasonably necessary in the circumstances based on information reviewed. However, one non-compliant disclosure by the RCMP represents the vast majority of all confirmed personal information that was disclosed under SCIDA in 2020.		disclosure would not affect any person's privacy interest more than was reasonably necessary in the circumstances. DND-CAF will assess the necessity of retaining the personal information received in light of any new information provided by the RCMP, NSIRA and the OPC's findings, and associated DND-CAF directives and policies. As indicated in the SCIDA report, DND/CAF received the information from the RCMP based on its counter-terrorism mandate.
4. NSIRA and the OPC recommend that the federal institutions listed in the Act avoid formulaic language in statements of accuracy and reliability when the nature and source of information disclosed is not derived from a routine process.	4. Almost all of the disclosures (nearly 98%) included accuracy and reliability statements, although there were inconsistencies with respect to the sufficiency and specificity of statements.	Agree	Several departments and agencies have existing internal policies which request that statements of accuracy and reliability be tailored to the specific disclosure and avoid the use of formulaic language. To further bolster this recommendation across federal institutions using the SCIDA to share information, Public Safety will update its SCIDA Guide, training and related guidance materials to reflect the fact that federal institutions should provide specific and clear statements of accuracy and reliability in circumstances where the information being disclosed is obtained through a non-routine process. Public Safety will equally encourage federal partners to include this guidance on statements of accuracy and reliability in their own internal policies where applicable.
5. NSIRA and the OPC recommend that institutions listed in Schedule 3 of the Act that request information from institutions not listed in SCIDA, inform the disclosing	5. The record keeping of one institution which used SCIDA for the first time did not meet the record-keeping requirements of the Act.	Agree	In the interest of furthering compliance with SCIDA among federal institutions, it is considered a best practice for requesting institutions listed in Schedule 3 of the Act to

NSIRA Recommendation	Related Findings(s)	Government Response	Explanation
<p>institution of their legal obligations with respect to disclosing information under the Act, including record-keeping requirements, and encourage the disclosing institution to seek advice from Justice Canada and Public Safety Canada.</p>			<p>inform disclosing institutions not listed in the SCIDA of their legal obligations with respect to any disclosures made under SCIDA, including record-keeping requirements. It is also considered a best practice for federal institutions to encourage partners that are not as familiar with the disclosure authorities under the SCIDA to seek out the resources available from the Department of Justice and Public Safety, as appropriate.</p> <p>While recognizing that these are best practices and not legal obligations of recipients, Public Safety will encourage partners to implement these best practices by including related guidance in its updated SCIDA guide.</p>
<p>6. NSIRA and the OPC recommend that federal institutions that routinely disclose or receive in accordance with the Act standardize their record keeping in accordance with the latest Public Safety guidance.</p>	<p>6. Most records were well organized with no discrepancies, although some were provided in a manner that was difficult to understand and review.</p>	<p>Agree</p>	<p>Several institutions have already, or are currently in the process of, standardizing their record-keeping policies to reflect the latest Public Safety guidance. Continued work through the Public Safety-led working groups will further help to bring record-keeping practices in line with standard guidelines for institutions that have yet to do so.</p> <p>Additionally, several partners have internal naming conventions or file reference systems which aid in record keeping standardization. Where such a system is not in place, Public Safety pioneered a common 'File Reference Number' system for institutions to use in their disclosures and receipts in the aim of standardizing their record keeping practices.</p>

NSIRA Recommendation	Related Findings(s)	Government Response	Explanation
<p>7. NSIRA and the OPC recommend that institutions ensure that records kept for bulk disclosures include an appropriately robust description of the information relied on to satisfy itself that the disclosure of all elements of the dataset meets section 5 of the Act, and that the level of internal oversight is commensurate with the privacy risk.</p>	<p>7. This review found instances where records kept for disclosures did not contain a sufficient description, as required under paragraph 9(1)(e), of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under this Act.</p>	<p>Agree</p>	<p>Records kept for bulk disclosures must contain sufficient information to demonstrate that the disclosure of all elements of the dataset meet the contribution and proportionality thresholds contained in the disclosure test of section 5 of the Act, and the level of internal oversight must be commensurate with the privacy risk. In certain cases, however, operational exigencies may require immediate action and follow-up oversight commensurate with the level of risk related to a threat that undermines the security of Canada.</p> <p>To assist departments and agencies in implementing this recommendation, further clarification from NSIRA and the OPC would be greatly appreciated regarding what constitutes an “appropriately robust description” of this information. Similarly, further clarification from NSIRA and the OPC on what constitutes a “bulk disclosure” would be equally appreciated as there is currently no standard Government of Canada definition for this term. Once these elements have been clarified, Public Safety will update the SCIDA guidance materials accordingly and share this information through their related interdepartmental working groups.</p>
<p>8. NSIRA and the OPC recommend that federal institutions include information about how the disclosure will contribute to their jurisdiction or responsibilities in respect of activities that undermine the security of Canada, and other information</p>	<p>7. This review found instances where records kept for disclosures did not contain a sufficient description, as required under paragraph 9(1)(e), of the information that was relied on to satisfy the disclosing institution that</p>	<p>Agree</p>	<p>Several institutions already include or request that information describing how the disclosure will contribute to recipient institutions’ jurisdiction or responsibilities in respect of activities that undermine the security of Canada be provided in writing. In order to</p>

NSIRA Recommendation	Related Findings(s)	Government Response	Explanation
<p>relevant to the disclosure test, in their written requests for information under the Act, even if this information was verbally communicated prior to the request to enable appropriate record keeping by disclosing institutions under SCIDA.</p>	<p>the disclosure was authorized under this Act.</p>		<p>assist in implementing this recommendation across all institutions, Public Safety will update its templates for requesting and disclosing information under the SCIDA to emphasize the importance of including this information in the written request or disclosure letter. Institutions which do not currently have a practice in place of including this information agree to review their internal policies in accordance with the updated SCIDA guidance materials once published.</p>
<p>9. NSIRA and the OPC recommend that IRCC and the CSE enter into an information-sharing arrangement that structures their disclosure of information under the Act.</p>	<p>8. NSIRA and the OPC found that almost all disclosures (over 97%) included caveats, which supported originator control and responsible information sharing.</p> <p>9. IRCC and CSE, as well as GAC and CSIS, regularly exchange information under SCIDA of a nature and in a manner that warrants information sharing arrangements, as encouraged by subsection 4(c) of the Act.</p>	<p>Agree</p>	<p>IRCC and the CSE will begin discussions to explore the best solutions for creating an information sharing agreement between both institutions that structures the disclosure of information under the SCIDA.</p>
<p>10. NSIRA and the OPC recommend that CSIS and GAC update their information-sharing arrangement, previously agreed upon under SCISA, to account for SCIDA.</p>	<p>8. NSIRA and the OPC found that almost all disclosures (over 97%) included caveats, which supported originator control and responsible information sharing.</p> <p>9. IRCC and CSE, as well as GAC and CSIS, regularly exchange information under SCIDA of a nature and in a manner that warrants information</p>	<p>Agree</p>	<p>CSIS and GAC will explore how best to update their information sharing agreement, previously agreed to under the SCISA, to account for the SCIDA. Both institutions will endeavour to begin the process of updating the information sharing arrangement within a reasonable timeframe and complete updates as soon as feasibly possible working within the constraints of existing priorities, emerging operational emergencies, and other complications which affect timelines.</p>

NSIRA Recommendation	Related Findings(s)	Government Response	Explanation
	sharing arrangements, as encouraged by subsection 4(c) of the Act.		
<p>11. NSIRA and the OPC recommend that the Canadian Food Inspection Agency consult Public Safety Canada, and develop and implement policies and procedures to support compliance with the Act.</p>	<p>10. NSIRA and the OPC found that Public Safety Canada coordinates the implementation of SCIDA among federal institutions, and that all 17 federal institutions listed in SCIDA have staff who have taken Public Safety Canada’s SCIDA training.</p> <p>11. NSIRA and the OPC found that the Canadian Food Inspection Agency did not have policies or procedures to support compliance with the Act.</p>	Agree	<p>Although the Canadian Food Inspection Agency (CFIA) has not yet disclosed or received information under the SCIDA, it will work collaboratively with Public Safety to develop and implement policies and procedures to support SCIDA compliance. CFIA staff will therefore feel empowered to disclose or receive national security information under the SCIDA should the need arise.</p>
<p>12. NSIRA recommends that Immigration, Refugees and Citizenship Canada and other institutions which routinely receive requests for information under SCIDA, put into written policy the practice of keeping information received in requests for information separate from the rest of its databanks and watch lists.</p>		Agree	<p>IRCC has an existing operational practice of separating requests for information from the rest of its databanks and watch lists. Although this practice is included in its Standard Operating Procedures document, for added clarity, IRCC will also add this policy into their Information Sharing Policy guide.</p> <p>Public Safety Canada will also include this guidance in its updated SCIDA guidance materials to encourage broader uptake of this best practice by other institutions which routinely receive requests for information under SCIDA.</p>