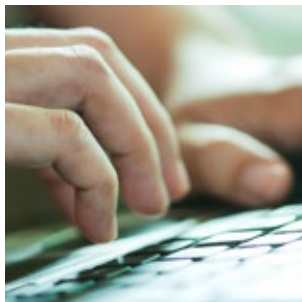


*Security of Canada  
Information Disclosure Act (SCIDA)*

**A Step-by-Step Guide  
to Responsible  
Information Sharing**



FOR OFFICIAL USE -  
NOT FOR FURTHER  
DISTRIBUTION

December 2019


BUILDING A **SAFE** AND **RESILIENT CANADA**



Public Safety  
Canada

Sécurité publique  
Canada

**Canada**



© Her Majesty the Queen in Right of Canada, 2019

Cat. No.: PS4-258/2019E-PDF

ISBN: 978-0-660-32647-4

# Table of Contents

Purpose.....	5
Background.....	5
Overview of the SCIDA.....	6
Steps for Institutions Disclosing Information under the SCIDA.....	8
Checklist for Institutions Disclosing Information under the SCIDA.....	9
Guide to the Checklist for Institutions Disclosing Information under the SCIDA.....	15
Steps for Institutions Receiving Information under the SCIDA.....	22
Checklist for Institutions Receiving Information under the SCIDA.....	23
Guide to the Checklist for Institutions Receiving Information under the SCIDA.....	27
Appendix A - Record-keeping Template for Institutions Disclosing Information under the SCIDA.....	31
Appendix B - Record-keeping Template for Institutions Receiving Information under the SCIDA.....	33
Appendix C - Government of Canada Institutions Authorized to Disclose Information under the SCIDA.....	35
Appendix D - National Security Mandates of the Designated Recipient Institutions under the SCIDA.....	41
Canada Border Services Agency.....	41
Canada Revenue Agency.....	43
Canadian Food Inspection Agency.....	44
Canadian Nuclear Safety Commission.....	44
Canadian Security Intelligence Service.....	46
Communications Security Establishment.....	48
Department of Immigration, Refugees and Citizenship Canada (Department of Citizenship and Immigration).....	52
Department of Finance.....	53

Global Affairs Canada (Department of Foreign Affairs).....	55
Department of Health.....	57
Department of National Defence / Canadian Armed Forces.....	58
Department of Public Safety and Emergency Preparedness.....	59
Department of Transport.....	63
Financial Transactions and Reports Analysis Centre of Canada.....	64
Public Health Agency of Canada.....	65
Royal Canadian Mounted Police.....	66
<b>Appendix E - Heads of the Designated Recipient Institutions and/or Person(s)</b>	
<b>Designated by them.....</b>	<b>69</b>
<b>Appendix F - <i>Security of Canada Information Disclosure Act</i>.....</b>	<b>77</b>

# Purpose

The purpose of this guide is to assist officials across the Government of Canada better understand how to navigate and use the *Security of Canada Information Disclosure Act* (SCIDA). The guide forms part of a larger information sharing toolkit designed by Public Safety Canada to support federal institutions in carrying out their responsibilities related to national security information sharing. It includes step-by-step instructions on how to share information under the SCIDA, as well as tools and tips to develop best practices in information sharing.

For questions about the guide and/or other SCIDA-related resources provided by Public Safety Canada's Strategic Coordination Centre on Information Sharing (SCCI), please send an email to: [ps.scci-ccsi.sp@canada.ca](mailto:ps.scci-ccsi.sp@canada.ca).

Public Safety Canada will continue to update this resource on a regular basis and distribute new versions as they become available.

# Background

The *Security of Canada Information Sharing Act* (SCISA), enacted in June 2015 as part of the *Anti-Terrorism Act* (former Bill C-51), was conceptualized in the context of a comprehensive reform of Canada's national security framework. This reform was the Government of Canada's (GOC) response to the findings in the 2004 and 2009 Status Reports of the Auditor General of Canada, the Reports of the Standing Committee on Public Accounts concerning those reports (2005 and 2009), the recommendations made by the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (2006) and the recommendations made by the Commission of Inquiry into the Investigation of the 1985 Bombing of Air India Flight 182 (2010).

The work of these commissions and bodies as well as public debate served to highlight the following realities about information sharing in Canada:

- In order to identify, assess and mitigate threats to national security, information from multiple departments and agencies must be drawn together;
- The efficient disclosure of information relating to national security threats is necessary for national security agencies to be effective; and,

- While government institutions share some information for national security purposes, there are barriers to optimal disclosure, such as:
  - complex legal frameworks that may cause confusion and fear;
  - some statutory regimes that may be overly restrictive; and,
  - an engrained culture of working in information silos.

In the fall of 2016, the Government of Canada launched extensive public consultations on possible reforms to Canada’s national security laws, including those concerning information sharing between Government of Canada institutions. Following the consultations, the Minister of Public Safety Canada introduced Bill C-59, *An Act respecting national security matters*, in June 2017. Bill C-59 proposed amendments to the provisions made by the former Bill C-51, including several amendments to the SCISA, the previous legislation for national security information sharing. After Bill C-59 received Royal Assent in June 2019 and became known as the *National Security Act*, the SCISA was amended and renamed the *Security of Canada Information Disclosure Act (SCIDA)*.

## Overview of the SCIDA

The SCIDA establishes an express, stand-alone authority for all GOC institutions to disclose national security related information, including personal information, either proactively or in response to a request, to GOC institutions with mandates to protect Canada against activities that undermine the security of Canada.

The SCIDA contains a number of noteworthy amendments that address concerns raised in relation to its predecessor, the SCISA. These include:

- replacement of the term “sharing” with the term “disclosure” to more accurately convey the purpose of the Act – the responsible disclosure of information in the possession of GOC institutions to ensure that information gets into the right hands, for the right reason;
- replacement of the standard of “relevance” with a higher two-part standard of contribution (whether the disclosure “contributes to” a national security mandate) and proportionality (whether its impact on the privacy of persons is minimized: i.e., the disclosure “must not affect any person’s privacy interest any more than reasonably necessary in the circumstances”);

- clarification that advocacy, protest, dissent or artistic expression are not considered activities that undermine the security of Canada, unless they are carried out in conjunction with an activity that undermines the security of Canada;
- a requirement on disclosing institutions to provide a statement on the accuracy of the information to be disclosed and the reliability of the manner in which the information was obtained;
- a requirement on recipient institutions to destroy or return any personal information that is not reasonably necessary in the circumstances; and
- a record-keeping obligation on every institution to create and retain a record of any information that is disclosed to or received by it, and for that institution to provide the National Security and Intelligence Review Agency (NSIRA) with a copy of that record.

Whether disclosure occurs proactively or in response to a request made by an institution that may receive information under the SCIDA, the SCIDA does not create an obligation to disclose information. The institution holding the information always retains the discretion to decide whether or not to disclose that information. Each Government institution's authority to collect, disclose, retain and use information (including personal information) also remains circumscribed by law, including the *Canadian Charter of Rights and Freedom (Charter)* and the *Privacy Act*. Importantly, the SCIDA does not take precedence over any other statutory or regulatory prohibitions or limitations on the disclosure of information.

The SCIDA also does not address **information collection**, which continues to be governed by existing lawful authorities, including the *Privacy Act* (e.g. with respect to the collection of personal information). It does not in any way expand the authority of a designated recipient to collect information that is disclosed to it under SCIDA.

# Steps for Institutions Disclosing Information under the SCIDA

Key Questions for Disclosing Institutions		
1.	Does your institution have information that you believe is linked to activities that undermine the security of Canada?	✓
2.	Is this disclosure prohibited or restricted by another federal statute or regulation?	✓
3.	Are you considering the disclosure of information to one of the designated recipient institutions?	✓
4.	Do you believe this information contributes to the recipient institution's national security mandate?	✓
5.	Does this information include any personal information?	✓
6.	Provide a statement on the accuracy and reliability of the information.	✓
7.	Disclosure of information.	✓
8.	Record of disclosure.	✓
9.	Report to the National Security and Intelligence Review Agency (NSIRA).	✓



# Checklist for Institutions Disclosing Information under the SCIDA

When you are considering the disclosure of information under the *Security of Canada Information Disclosure Act* (SCIDA), you may find it helpful to use this checklist. If, **after completing all steps below**, you determine that the disclosure of information under the SCIDA is indeed authorized and appropriate, you should create and retain a record of your determination and the reasons for it. A record-keeping template for institutions disclosing information under the SCIDA can be found in **Appendix A** to the Guide.

If you cannot complete all of the steps in this checklist, then the disclosure of information may not be authorized under the SCIDA. If, at any point, you determine that the disclosure of information under the SCIDA is not authorized or appropriate, it is also good practice to create and retain a record for review purposes (e.g., email, memo to file).

Name of Disclosing Institution: \_\_\_\_\_

## STEP 1: Does your institution have information that you believe is linked to activities that undermine the security of Canada?

**(a) Provide a brief description of the information to be disclosed (exclude specific details).**

*The SCIDA defines an activity that undermines the security of Canada as any activity that undermines the sovereignty, security or territorial integrity of Canada or threatens the lives or the security of people in Canada or of any individual who has a connection to Canada and who is outside Canada.*

**CONSIDER:** If your answer is **no**, stop here and do not disclose the information.

**(b) Indicate the type of activity the information relates to (check all that apply):**

- Interference with the capability of the Government of Canada in relation to intelligence, defence, border operations or public safety
- Changing or unduly influencing a government in Canada by force or unlawful means
- Espionage, sabotage or covert foreign-influenced activities
- Terrorism
- Proliferation of nuclear, chemical, radiological or biological weapons
- Significant or widespread interference with critical infrastructure
- Significant or widespread interference with the global information structure, defined as electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in, or relating to those emissions, systems, or networks
- Conduct that takes place in Canada and that undermines the security of another state
- Other (i.e., **any other activity** that undermines the security of Canada but is not listed above):

---

GO TO [NOTE 1](#)

**NOTE:** Information related to the activities of **advocacy, protest, dissent or artistic expression does not fall within the scope of the definition** of an activity that “undermines the security of Canada” **unless it is carried out in conjunction with an activity listed in 1(b).**

**STEP 2: Is this disclosure prohibited or restricted by another federal statute or regulation?**

- Yes, the ability to disclose this information is prohibited or restricted by other legislation. **(Therefore, the disclosure of this information may not be authorized under the SCIDA.)**
- No, the ability to disclose this information is not prohibited or restricted by other legislation.

GO TO [NOTE 2](#)

**CONSIDER:** If your answer is yes, stop here and do not disclose the information.

### STEP 3: Are you considering the disclosure of information to one of the designated recipient institutions?

- Canada Border Services Agency
- Canada Revenue Agency
- Canadian Food Inspection Agency
- Canadian Nuclear Safety Commission
- Canadian Security Intelligence Service
- Communications Security Establishment
- Immigration, Refugees and Citizenship Canada
- Finance Canada
- Global Affairs Canada
- Health Canada
- Department of National Defence / Canadian Armed Forces<sup>1</sup>
- Public Safety Canada
- Transport Canada
- Financial Transactions and Reports Analysis Centre of Canada
- Public Health Agency of Canada
- Royal Canadian Mounted Police

GO TO [NOTE 3](#)

---

<sup>1</sup> While the Department of National Defence (DND) and the Canadian Armed Forces (CAF) are separate entities, they share the same national security mandate. For each institution's contact details, refer to [Appendix E](#).

**CONSIDER:** If your answer is **no**, stop here and do not disclose the information.

#### STEP 4: Do you believe this information contributes to the recipient institution's national security mandate?

Provide a description of **how you believe this information will contribute** to the recipient institution's national security mandate (i.e., its jurisdiction or responsibilities).

GO TO [NOTE 4](#)

**CONSIDER:** If your answer is **no**, stop here and do not disclose the information.

#### STEP 5: Does this information include any personal information?

- No, this information does not include any personal information.
- Yes, this information does include personal information, but any information that is not reasonably necessary in the circumstances to include has been removed. The personal information that has been removed will not be disclosed to the recipient institution.

GO TO [NOTE 5](#)

## STEP 6: Provide a statement on the accuracy and reliability of the information.

Provide a statement on both the **accuracy** of the information and the **reliability** of the manner in which this information was obtained.

GO TO [NOTE 6](#)

## STEP 7: Disclosure of information.

Date of disclosure (mm/dd/yyyy): \_\_\_\_\_

**This disclosure is authorized by the following:**

Name/Position: \_\_\_\_\_

Branch/Division: \_\_\_\_\_

**This information is being disclosed to the following:**

Name of Institution: \_\_\_\_\_

GO TO [NOTE 7](#)

## STEP 8: Record of disclosure.

- ❑ A copy of your record of the disclosure has been created and contains the following:
  - a description of the information;
  - the name of the individual who authorized its disclosure;
  - the name of the recipient Government of Canada institution;
  - the date on which the information was disclosed;
  - a description of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under the SCIDA; and,
  - any other information specified by the regulations.

GO TO [NOTE 8](#)

## STEP 9: Report to the National Security and Intelligence Review Agency (NSIRA).

- ❑ You have undertaken the appropriate steps to ensure that a record of the disclosure is provided to the National Security and Intelligence Review Agency (NSIRA) within 30 days of the end of the calendar year (January 30<sup>th</sup>).

GO TO [NOTE 9](#)

# Guide to the Checklist for Institutions Disclosing Information under the SCIDA

## STEP 1: Does your institution have information that you believe is linked to activities that undermine the security of Canada?

- The types of activities listed in Step 1(b) are illustrative examples of activities from the SCIDA definition. Since this list of activities is not exhaustive, institutions may identify information for disclosure that involves other activities that undermine the security of Canada.
- In your description, you may find it helpful to use key words that speak to the categories or types of information involved, such as reports, interviews, operational notes, assessments, photographs, emails, memoranda, letters, audio-visual recordings, social media, and so on.
- Prior to disclosure, you are strongly encouraged to communicate with the designated recipient institution to clarify whether the information is indeed linked to activities that undermine the security of Canada and, if so, how that information contributes to the designated recipient institution's national security mandate, as explained in [Step 4](#). During these discussions, you should only provide enough information to determine whether you are disclosing the right information to the right institution for the right reasons. Refer to [Appendix D](#) for a description of the designated recipient institutions' national security mandates.
- Informal communication should not be used in lieu of the formal disclosure process or to replace the formal record-keeping obligations. It is recommended that correspondence regarding a requested disclosure be retained for your institution's records.

**NOTE:** A government institution may disclose information believed to be linked to an activity that undermines the security of Canada, **even if this information was collected for a purpose other than national security** (provided that all of the requirements of the SCIDA have been met). In other words, the disclosure authority provided under the SCIDA is not limited to information that was initially collected for national security purposes.

## STEP 2: Is this disclosure prohibited or restricted by another federal statute or regulation?

- The SCIDA provides a stand-alone authority for the disclosure of information related to the security of Canada where no such explicit authority exists; it does not replace or take precedence over existing statutory or regulatory authorities on the disclosure of information.
- If any legislation or regulations, other than the SCIDA, prohibit the disclosure of the information entirely, then the information may not be disclosed. If any legislation or regulations, other than the SCIDA, impose restrictions or additional requirements to the disclosure of the information, then those restrictions and requirements must be followed when the information is disclosed.
  - For example, the *Department of Employment and Social Development Act* (DESDA) puts limitations on how the Department of Employment and Social Development Canada (ESDC) may disclose personal information. As the SCIDA does not supersede or override existing legislation, ESDC must follow the information scheme found in the DESDA. This means that ESDC cannot rely on the SCIDA to disclose personal information.

**NOTE:** If you are uncertain about whether you are authorized to disclose information, it is recommended that you consult with your manager, Departmental Legal Services Unit, Information Technology (IT) Services, Chief Information Officer (CIO) and/or Access to Information and Privacy (ATIP) Office for advice on how best to proceed.

## STEP 3: Are you considering the disclosure of information to one of the designated recipient institutions listed?

- To determine whether your institution is authorized to disclose information under the SCIDA, you should confirm that it is a Government of Canada institution listed in [Appendix C](#).
- If your institution is authorized to disclose information under the SCIDA, you may disclose to the institutions listed under Schedule 3 of the SCIDA. Refer to [Appendix D](#) for a list of the designated recipient institutions, as well as a description of their national security mandates.



- In the event that you are disclosing the same information to more than one designated recipient institution at the same time, you should complete a separate disclosure for each institution by completing a separate checklist and creating and retaining a separate record.

### Privacy Considerations:

- If your institution is likely to disclose information with other departments and agencies on a regular basis, it is recommended that you prepare an information sharing agreement (ISA) to govern that relationship – and help protect any personal information.
- ISAs are useful for establishing common policies, practices and controls.
- ISAs should, at a minimum:
  - define the specific elements of personal information to be shared;
  - define the specific purposes for the sharing; and
  - limit secondary uses and onward transfer.

### STEP 4: Do you believe this information contributes to the recipient institution’s national security mandate?

- In order to strike a balance between furthering the important national security objectives of the SCIDA and respecting the individual privacy rights of Canadians, the SCIDA requires that the disclosed information **contribute to the national security mandate of a designated recipient institution**. The information must not only be “relevant to” the recipient institution’s mandate in relation to the security of Canada (which was the previous threshold under the SCISA), but it must “contribute to” that mandate. You may wish to consider the following questions in making that determination:
  - Will the information provide background on activities that undermine the security of Canada, the extent of those activities, or other possible avenues of investigative inquiry for that institution?
  - Will it help that institution identify key individuals engaged in those activities?
- As described in [Step 1](#), you are encouraged 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 contributes to that institution’s national security mandate. Refer to [Appendix D](#) for a description of the designated recipient institutions’ national security mandates.

## STEP 5: Does this information include any personal information?

- Personal information includes any identifiable information about an individual, such as, but not limited to, name, age, marital status, race, national or ethnic origin, religion, education, address, fingerprints, blood type, and medical, criminal, or employment history (for more information about what counts as personal information, refer to section 3 of the [Privacy Act](#)).
- It is important to note that “personal information” in the context of the SCIDA includes information about corporations.
- Before information can be disclosed, you must be satisfied that the disclosure will not impact a person’s privacy interests any more than is **reasonably necessary in the circumstances**. Any information that would impact a person’s privacy interests more than reasonably necessary in the circumstances must be removed before the disclosure takes place. Your institution should tailor each disclosure so that only what is reasonable necessary is provided. Including less personal information can help reduce the risk of inappropriate use, disclosure and loss.
- Whether the information impacting an 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 disclosure.
- Establishing a dialogue early on with the designated recipient institution will assist you in determining what is reasonably necessary for the disclosure.

**NOTE:** If you are uncertain as to whether information is reasonably necessary in the circumstances, it is recommended that you consult with your manager, Departmental Legal Services Unit, Chief Information Officer (CIO) and/or Access to Information and Privacy (ATIP) Office for advice on how best to proceed.

### Privacy Considerations:

- If your institution is expected to disclose personal information under the SCIDA, you should consider whether a formal assessment of its associated privacy impacts is warranted and whether a privacy impact assessment (PIA) needs to be updated. A PIA can help to manage risk and is useful for making good decisions and maintaining accountability.

- The increased volume and type of information disclosed and/or received under the SCIDA, as well as the disclosure of information for purposes other than that for which it was collected, could constitute a substantial modification to an institution's regular programs or activities, thus triggering the need to possibly establish a new PIA or update an existing one to the extent that the SCIDA impacts the manner in which information is collected, used or disclosed.
- Consult with your Access to Information and Privacy (ATIP) Office for PIA-related inquiries.

## STEP 6: Provide a statement on the accuracy and reliability of the information.

- At the time of disclosure, a statement must be provided that addresses the accuracy of the information as well as the reliability of the manner in which it was obtained. Ensuring that the information is as accurate, complete and as up-to-date as possible is key to responsible and effective disclosures.
  - Any concerns regarding the accuracy or reliability of the manner in which the information was obtained must be clearly conveyed to the designated recipient institution.
- In order to determine the **accuracy** of the information, the following should be considered:
  - Does your institution have any reason to believe that this information could be inaccurate?
  - Is there any evidence to support the accuracy of this information?
  - Has your institution independently verified this information?
- In order to determine the **reliability** of the manner in which the information was obtained, the following questions should be considered:
  - Was the information to be disclosed obtained in a reliable manner or from a reliable source? As an example, if the information was obtained as a result of torture, it is reasonable to believe that it was obtained in an unreliable manner and could be inaccurate.
  - Has your institution verified the reliability of the manner in which this information was obtained?
  - Has your institution previously held information that was obtained in this same manner? If so, was it reliable?

## Privacy Considerations:

- When disclosing personal information, you should ensure that it is as accurate, complete, and as up-to-date as possible to minimize the possibility that incorrect information is used to make a decision about an individual.
- Any corrections that have been previously made or requested in relation to personal information should be included as part of the statement of accuracy.

## STEP 7: Disclosure of information.

- Information may only be disclosed to the head of a designated recipient institution or persons who have been designated by the head to receive information under the SCIDA. This ensures that only those who require the information to fulfil their mandates receive the information. For a list of designated heads or persons, refer to [Appendix E](#).
- To facilitate good record-keeping, it is recommended that you include as much information as possible about the persons who authorized the disclosure and received the information **unless the disclosure of that information would result in a risk to an ongoing investigation or to whoever is disclosing/receiving the information**. This will facilitate follow-up after the fact if questions or concerns arise between the disclosing and the recipient institutions.
- It is good practice to consider imposing **caveats** on disclosures of information undertaken pursuant to the SCIDA. For example, a disclosing institution may include caveats such as: “The information is prohibited from further disclosure to any recipient not listed as a designated recipient institution under the SCIDA, without prior written consent; the information is not to be used for purposes other than the reason for which it was shared; the information must be destroyed after a set period of time.”
- While caveats can help the disclosing institution safeguard information, they are not a legal requirement. There are circumstances that may supersede imposed caveats, such as:
  - when further disclosure is required by law;
  - when further disclosure is authorized by law; and/or,
  - when situations or exigent circumstances that would make the obtaining the consent impracticable or unfeasible (i.e. threat is imminent).

## Privacy Considerations:

- It is important that caveats be precise so that expectations are clear to the recipient institution.
- Possible future disclosures should be a factor in assessing whether to disclose the information to a recipient institution. Such an assessment should also inform the content of the caveats.

## STEP 8: Record of disclosure.

- Every Government of Canada institution authorized to disclose under the SCIDA must create and retain a record of each disclosure of information.
- You may wish to use the record-keeping template found in [Appendix A](#). This template will help you satisfy the record-keeping obligation under the SCIDA.
- If your institution has chosen not to use the record-keeping template, then you must ensure that your institution keeps a record of the following information:
  - a description of the information;
  - the name of the individual who authorized its disclosure;
  - the name of the recipient Government of Canada institution;
  - the date on which the information was disclosed;
  - a description of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under the SCIDA; and,
  - any other information specified by the regulations.

**NOTE:** It is important to remember to sign the record of disclosure and provide a copy of it to the appropriate person in your institution so it can be retained for reporting purposes. A standardized process for record keeping is highly recommended for all disclosing institutions sharing information under the SCIDA.

## STEP 9: Report to the National Security and Intelligence Review Agency (NSIRA).

- A copy of each record produced by a disclosing institution must be provided to the National Security and Intelligence Review Agency (NSIRA) within 30 days after the end of the calendar year (January 30<sup>th</sup>).

# Steps for Institutions Receiving Information under the SCIDA

## Key Questions for Recipient Institutions

1.	Has your institution received information pursuant to the SCIDA?	✓
2.	Which institution disclosed this information to your institution?	✓
3.	To whom in your institution was this information disclosed?	✓
4.	Does this information include any personal information?	✓
5.	Record of receipt.	✓
6.	Report to the National Security and Intelligence Review Agency (NSIRA).	✓

# Checklist for Institutions Receiving Information under the SCIDA

Prior to requesting or receiving information under the *Security of Canada Information Disclosure Act* (SCIDA), you may find it helpful to use this checklist. If, after completing all steps below, you determine that the receipt of information under the SCIDA is indeed authorized and appropriate, you should create and retain a record of your determination and the reasons for it. A record-keeping template for institutions receiving information under the SCIDA can be found in **Appendix B** to the Guide.

If you cannot complete all of the steps in this checklist, then the receipt of information may not be authorized under the SCIDA. If, at any point, you determine that the receipt of information under the SCIDA is not authorized or appropriate, it is recommended that you destroy or return the information to the disclosing institution and create and retain a record for review purposes (e.g., email, memo to file).

Name of Recipient Institution: \_\_\_\_\_

## STEP 1: Has your institution received information pursuant to the SCIDA?

**(a) Provide a brief description of the information received (exclude specific details):**

*The SCIDA defines an activity that undermines the security of Canada as any activity that undermines the sovereignty, security or territorial integrity of Canada or threatens the lives or the security of people in Canada or of any individual who has a connection to Canada and who is outside Canada.*

GO TO [NOTE 1](#)

**NOTE:** Information related to the activities of **advocacy, protest, dissent or artistic expression does not fall within the scope of the definition** of an activity that “undermines the security of Canada” **unless it is carried out in conjunction with an activity listed in 1(b).**

## STEP 2: Which institution disclosed this information to your institution?

**This information was disclosed by the following:**

Name of Institution: \_\_\_\_\_

GO TO [NOTE 2](#)

## STEP 3: To whom in your institution was this information disclosed?

Date of receipt (mm/dd/yyyy): \_\_\_\_\_

**This information was received by the following:**

Head of the institution

**OR**

Designated person

Name/Position: \_\_\_\_\_

Branch/Division: \_\_\_\_\_

GO TO [NOTE 3](#)



## STEP 4: Does this information include any personal information?

No, this information does not include any personal information.

Yes, this information does include personal information, but it is necessary for my institution to carry out its national security mandate.

OR

Yes, this information does include personal information, but it is not necessary for my institution to carry out its national security mandate, and **it has been destroyed or returned**.

OR

Yes, this information does include personal information that is not necessary for my institution to carry out its national security mandate, but **it has been retained** in accordance with the following authority:

---

GO TO [NOTE 4](#)

**NOTE:** Where you determine that only part of the personal information is necessary for your institution to carry out its national security mandate, it is important that you **return or destroy the personal information** that is not necessary for that purpose.

## STEP 5: Record of receipt

- ❑ A copy of your record of the receipt has been created and contains the following information:
  - a description of the information;
  - the name of the head of the institution or designated person who received it;
  - the name of the disclosing Government of Canada institution;
  - the date on which the information was received;
  - whether personal information that is not necessary for the recipient institution to carry out its responsibilities has been destroyed or returned;
  - if the information was destroyed, the date on which it was destroyed;
  - if the information was returned, the date on which it was returned; and,
  - any other information specified by the regulations.

GO TO [NOTE 5](#)

## STEP 6: Report to the National Security and Intelligence Review Agency (NSIRA)

- ❑ You have undertaken the appropriate steps to ensure that a record of the disclosure is provided to the National Security and Intelligence Review Agency (NSIRA) within 30 days after the end of the calendar year (January 30<sup>th</sup>).

GO TO [NOTE 6](#)

# Guide to the Checklist for Institutions Receiving Information under the SCIDA

## STEP 1: Has your institution received information that you believe is linked to activities that undermine the security of Canada?

- The types of activities listed in Step 1 are illustrative examples of activities from the SCIDA definition. Since this list of activities is not exhaustive, institutions may identify information for disclosure that involves other activities that undermine the security of Canada.
- Prior to receiving any information, it is important to confirm that your institution is one of the listed recipients in Schedule 3 of the SCIDA (refer to [Appendix C](#)). If your institution is not listed it cannot receive information under the SCIDA. In these cases, you will need to consider another authority to obtain the required information.
- In the event that you have requested information from the disclosing institution, it is strongly recommended that you communicate with them to discuss your request prior to any disclosure taking place. This dialogue will help the disclosing institution better understand the purpose of your request and the relevant parts of your institution's national security mandate, which will ultimately assist them in determining what information can be disclosed. During these discussions, you should provide enough information to help the disclosing institution determine whether the information in their possession should be disclosed to your institution.
- Informal communication should not be used in lieu of the formal disclosure process or to replace the formal record-keeping obligations. All correspondence regarding a requested disclosure should be retained for your institution's records.
- In the event that you have been provided with a proactive disclosure of information, some of the preliminary steps in this checklist may not apply. Nevertheless, it is recommended that you include as much information as possible about the persons who authorized the disclosure and received the information **unless the disclosure of that information would result in a risk to an ongoing investigation or to whoever is receiving the information**. It is also good practice to ensure that any personal information included in the disclosure is appropriate and is properly handled, as described in [Step 4](#).

## STEP 2: Which institution disclosed this information to your institution?

- To satisfy the record-keeping obligations imposed on your institution by the SCIDA, you need to keep a record of which institution that disclosed the information to you. For a more complete record-keeping practice, make sure to fill out as much information as possible in [Step 3](#).
- To verify whether the disclosing institution is a Government of Canada institution authorized to disclose information under the SCIDA, refer to [Appendix C](#).

### Privacy Considerations:

- If your institution is likely to receive information with other departments and agencies on a regular basis, it is recommended that you prepare an information sharing agreement (ISA) to govern that relationship – and protect any personal information.
- ISAs are useful for establishing common policies, practices and controls.
- ISAs should, at a minimum:
  - define the specific elements of personal information to be shared;
  - define the specific purposes for the sharing; and,
  - limit secondary uses and onward transfer.

## STEP 3: To whom in your institution was this information disclosed?

- Information may only be disclosed to the head of a designated recipient institution or those who have been designated the responsibility to receive information under SCIDA. This requirement is to ensure that only those who require the information to fulfill their mandate receive the information. For a list of designated heads and/or persons, refer to [Appendix E](#).
- Disclosures undertaken pursuant to the SCIDA may be subject to **caveats**. It is recommended that you communicate with the disclosing institution to ensure that all caveats imposed on the information can be respected. If your institution cannot comply with any of these imposed caveats, you should advise the disclosing institution immediately and the information should be returned, destroyed or otherwise dealt with as requested.

- While caveats can help the disclosing institution safeguard information, they are not a legal requirements, and there are circumstances that may supersede imposed caveats, such as:
  - when further disclosure is required by law;
  - when further disclosure is authorized by law; and/or,
  - when situations or exigent circumstances that would make the obtaining the consent impracticable or unfeasible (i.e. threat is imminent).

#### STEP 4: Does this information include any personal information?

- Personal information includes any identifiable information about an individual, such as, but not limited to, name, age, marital status, race, national or ethnic origin, religion, education, address, fingerprints, blood type, and medical, criminal, or employment history (for more information about what counts as personal information, refer to section 3 of the *Privacy Act*).
- While the SCIDA authorizes the disclosure of personal information, it also imposes an obligation on the recipient institution to identify, as soon as feasible after receipt, any personal information that may have been disclosed to it. Any personal information that is not necessary to your institution's ability to carry out its national security mandate must be destroyed or returned to the disclosing institution.
- Before destroying or returning any unnecessary personal information, your institution should evaluate whether there are exceptions or legal requirements to keep it. For example, the requirement to destroy or return personal information does not apply to:
  - Information subject to requests under the *Access to Information Act*, the *Library and Archives of Canada Act*, or the *Privacy Act*;
  - Certain law enforcement institutions, like the Royal Canadian Mounted Police (RCMP), if they are subject to a criminal law disclosure obligation; and,
  - The Canadian Security Intelligence Service (CSIS) if the information is relevant to the performance of its duties under s. 12 of the *Canadian Security Intelligence Service Act*.
- As described in [Step 1](#), you are encouraged to communicate with the disclosing institution prior to disclosure so that they understand why the personal information is needed and how it contributes to your institution's national security mandate. Identifying and clearly articulating the details of the information being requested will assist the disclosing institution in determining whether the information can be disclosed to you and help avoid the disclosure of unnecessary information, particularly of unnecessary personal information.

## STEP 5: Record of receipt.

- Every Government of Canada institution receiving information under the SCIDA must create and retain a record of each disclosure of information.
- You may wish to use the record-keeping template found in [Appendix B](#). This template will help you satisfy the record-keeping obligation under the SCIDA.
- If your institution has chosen not to use the record-keeping template, then you must ensure that your institution keeps a record of the following information:
  - a description of the information;
  - the name of the individual who authorized its receipt;
  - the name of the disclosing Government of Canada institution;
  - the date on which the information was received;
  - whether personal information that is not necessary for your institution to carry out its responsibilities has been destroyed or returned;
  - if the information was destroyed, the date on which it was destroyed;
  - if the information was returned, the date on which it was returned; and,
  - any other information specified by the regulations.

**NOTE:** It is important to sign the record of receipt and provide a copy of it to the appropriate person in your institution so it can be retained for reporting purposes. A standardized process for record keeping is recommended for all recipient institutions sharing information under the SCIDA.

## STEP 6: Report to the National Security and Intelligence Review Agency (NSIRA).

- A copy of each record produced by a recipient institution must be provided to the National Security Intelligence and Review Agency (NSIRA) within 30 days after the end of the calendar year (January 30<sup>th</sup>).

# Appendix A

## Record-keeping Template for Institutions Disclosing Information under the SCIDA

A record of all disclosed information must be provided to the National Security and Intelligence Review Agency (NSIRA) **within 30 days after the end of each calendar year** (January 30<sup>th</sup>). Completing this template will help you meet the record-keeping obligations for disclosing institutions under the SCIDA.

<b>File Reference Number:</b>
<b>Name of your institution<sup>2</sup>:</b>
<b>Name and position of the individual who authorized the disclosure of this information:</b>

---

2 It is recommended that the format used for the File Reference Number be as follows: (year / disclosing institution acronym / recipient institution acronym / four-digit unique identifier). The unique identifier should be a four-digit number generated by the disclosing institution for every disclosure that is made (e.g., 2019/RCMP/CSIS/0001).

<b>Provide a brief description of the information to be disclosed (without specific details):</b>
<b>Name of the recipient Government of Canada institution to which you are disclosing:</b>
<b>Name of the head of the recipient institution, or name and position of the designated person, to whom you are disclosing this information:</b>
<b>Describe the information that was relied on to satisfy you that the disclosure was authorized under this Act<sup>3</sup>:</b>
<b>The date on which this information was disclosed:</b>

---

3 According to s. 5.1 of the SCIDA, a disclosure is authorized if you are satisfied that a) it will contribute to the recipient institution's national security mandate, and that b) it will not affect any person's privacy interest more than is reasonably necessary in the circumstances.



# Appendix B

## Record-keeping Template for Institutions Receiving Information under the SCIDA

A record of all received information must be provided to the National Security and Intelligence Review Agency (NSIRA) **within 30 days after the end of each calendar year** (January 30<sup>th</sup>). Completing this template will help you meet the record-keeping obligations for receiving institutions under the SCIDA.

<b>File Reference Number<sup>4</sup>:</b>
<b>Name of your institution:</b>
<b>Name and position of the individual who received this information:</b>

---

4 It is recommended that the format used for the File Reference Number be as follows: (year / disclosing institution acronym / recipient institution acronym / four-digit unique identifier). The unique identifier should be a four-digit number generated by the disclosing institution for every disclosure that is made (e.g., 2019/RCMP/CSIS/0001).

**Provide a brief description of the information received (without specific details):**

**Name of the Government of Canada institution that disclosed this information:**

**Name and position of the individual who authorized the disclosure of this information:**

**The date on which this information was received:**

**If any personal information was destroyed or returned:**

- The personal information was destroyed on (mm/dd/yyyy): \_\_\_\_\_
- The personal information was returned on (mm/dd/yyyy): \_\_\_\_\_

# Appendix C

## Government of Canada Institutions Authorized to Disclose Information under the SCIDA

This list reproduces the *Privacy Act* definition of “government institution” and is intended for reference purposes only. It is entirely possible that an institution listed below may be associated with a different name or no longer exists.

### Departments and Ministries of State

- Department of Agriculture and Agri-Food
- Department of Canadian Heritage
- Department of Citizenship and Immigration
- Department of Employment and Social Development
- Department of the Environment
- Department of Finance
- Department of Fisheries and Oceans
- Department of Foreign Affairs, Trade and Development
- Department of Health
- Department of Indian Affairs and Northern Development
- Department of Industry
- Department of Justice
- Department of National Defence (including the Canadian Forces)
- Department of Natural Resources
- Department of Public Safety and Emergency Preparedness
- Department of Public Works and Government Services
- Department of Transport
- Department of Veterans Affairs
- Department of Western Economic Diversification

### Other Government Institutions

- Administrative Tribunals Support Service of Canada
- Asia-Pacific Foundation of Canada

- Atlantic Canada Opportunities Agency
- Belledune Port Authority
- British Columbia Treaty Commission
- Canada Border Services Agency
- Canada Emission Reduction Incentives Agency
- Canada Employment Insurance Commission
- Canada Foundation for Innovation
- Canada Foundation for Sustainable Development Technology
- Canada–Newfoundland and Labrador Offshore Petroleum Board
- Canada–Nova Scotia Offshore Petroleum Board
- Canada Revenue Agency
- Canada School of Public Service
- Canadian Advisory Council on the Status of Women
- Canadian Centre for Occupational Health and Safety
- Canadian Environmental Assessment Agency
- Canadian Food Inspection Agency
- Canadian Government Specifications Board
- Canadian Grain Commission
- Canadian Human Rights Commission
- Canadian Institutes of Health Research
- Canadian Museum for Human Rights
- Canadian Museum of Immigration at Pier 21
- Canadian Northern Economic Development Agency
- Canadian Nuclear Safety Commission
- Canadian Polar Commission
- Canadian Radio-television and Telecommunications Commission
- Canadian Security Intelligence Service
- Canadian Space Agency
- Canadian Transportation Accident Investigation and Safety Board
- Canadian Transportation Agency
- Canadian Wheat Board
- Civilian Review and Complaints Commission for the Royal Canadian Mounted Police
- Communications Security Establishment
- Copyright Board
- Correctional Service of Canada
- Director of Soldier Settlement
- The Director, *The Veterans' Land Act*

- Economic Development Agency of Canada for the Regions of Quebec
- Energy Supplies Allocation Board
- Federal Economic Development Agency for Southern Ontario
- Federal-Provincial Relations Office
- Federal Public Service Health Care Plan Administration Authority
- Financial Consumer Agency of Canada
- Financial Transactions and Reports Analysis Centre of Canada
- First Nations Financial Management Board
- First Nations Tax Commission
- Gwich'in Land and Water Board
- Gwich'in Land Use Planning Board
- Halifax Port Authority
- Hamilton Port Authority
- Historic Sites and Monuments Board of Canada
- Immigration and Refugee Board
- Indian Residential Schools Truth and Reconciliation Commission
- Law Commission of Canada
- Library and Archives of Canada
- Mackenzie Valley Environmental Impact Review Board
- Mackenzie Valley Land and Water Board
- Military Grievances External Review Committee
- Military Police Complaints Commission
- Montreal Port Authority
- Nanaimo Port Authority
- The National Battlefields Commission
- National Energy Board
- National Farm Products Council
- National Film Board
- National Research Council of Canada
- Natural Sciences and Engineering Research Council
- Northern Pipeline Agency
- Nunavut Surface Rights Tribunal
- Nunavut Water Board
- Office of Infrastructure of Canada
- Office of Privatization and Regulatory Affairs
- Office of the Administrator of the Ship-source Oil Pollution Fund
- Office of the Auditor General of Canada

- Office of the Chief Electoral Officer
- Office of the Commissioner of Lobbying
- Office of the Commissioner of Official Languages
- Office of the Communications Security Establishment Commissioner
- Office of the Comptroller General
- Office of the Co-ordinator, Status of Women
- Office of the Correctional Investigator of Canada
- Office of the Director of Public Prosecutions
- Office of the Information Commissioner
- Office of the Privacy Commissioner
- Office of the Public Sector Integrity Commissioner
- Office of the Superintendent of Financial Institutions
- Oshawa Port Authority
- Parks Canada Agency
- Parole Board of Canada
- Patented Medicine Prices Review Board
- Petroleum Compensation Board
- The Pierre Elliott Trudeau Foundation
- Port Alberni Port Authority
- Prairie Farm Rehabilitation Administration
- Prince Rupert Port Authority
- Privy Council Office
- Public Health Agency of Canada
- Public Service Commission
- Quebec Port Authority
- Regional Development Incentives Board
- Royal Canadian Mounted Police
- Royal Canadian Mounted Police External Review Committee
- Saguenay Port Authority
- Sahtu Land and Water Board
- Sahtu Land Use Planning Board
- Saint John Port Authority
- Security Intelligence Review Committee
- Sept-Îles Port Authority
- Shared Services Canada
- Social Sciences and Humanities Research Council
- Statistics Canada

- Statute Revision Commission
- St. John's Port Authority
- Thunder Bay Port Authority
- Toronto Port Authority
- Treasury Board Secretariat
- Trois-Rivières Port Authority
- Vancouver Fraser Port Authority
- Veterans Review and Appeal Board
- Windsor Port Authority
- Yukon Environmental and Socio-economic Assessment Board
- Yukon Surface Rights Board

## Crown Corporations

- Atlantic Pilotage Authority
- Atomic Energy of Canada Limited
- Bank of Canada
- Blue Water Bridge Authority
- Business Development Bank of Canada
- Canada Council<sup>3</sup> for the Arts
- Canada Deposit Insurance Corporation
- Canada Development Investment Corporation
- Canada Lands Company Limited
- Canada Mortgage and Housing Corporation
- Canada Pension Plan Investment Board
- Canada Post Corporation
- Canadian Air Transport Security Authority
- Canadian Broadcasting Corporation
- Canadian Commercial Corporation
- Canadian Dairy Commission
- Canadian Museum of Civilization
- Canadian Museum for Human Rights
- Canadian Museum of Immigration at Pier 21
- Canadian Museum of Nature
- Canadian Race Relations Foundation
- Canadian Tourism Commission
- Corporation for the Mitigation of Mackenzie Gas Project Impacts
- Defence Construction (1951) Limited

- Enterprise Cape Breton Corporation
- Export Development Canada
- Farm Credit Canada
- Federal Bridge Corporation Limited, The
- Freshwater Fish Marketing Corporation
- Great Lakes Pilotage Authority
- International Development Research Centre
- Laurentian Pilotage Authority
- Marine Atlantic Inc
- National Arts Centre Corporation
- National Capital Commission
- National Gallery of Canada
- National Museum of Science and Technology
- Old Port of Montreal Corporation Inc
- Pacific Pilotage Authority
- Parc Downsview Park Inc
- PPP Canada Inc.
- Public Sector Pension Investment Board
- Ridley Terminals Inc
- Royal Canadian Mint
- Standards Council of Canada
- Telefilm Canada
- VIA Rail Canada Inc



# Appendix D

## National Security Mandates of the Designated Recipient Institutions under the SCIDA

For reference, and to assist you as a representative of a Government of Canada disclosing institution, this Appendix lists all designated recipient institutions identified in Schedule 3 under the SCIDA. Below is a description of each institution’s national security mandate – its jurisdiction or responsibilities in respect of activities that undermine the security of Canada – as well as the relevant Act of Parliament or other lawful authorities under which that mandate is exercised.

### Canada Border Services Agency

The Canada Border Services Agency (CBSA) is responsible for providing integrated border services that support national security and public safety priorities, and for facilitating the free flow of people and goods – including animals and plants – across the border. It does this by administering and enforcing its program legislation, immigration and customs related statutes, as well as several other statutes on the behalf of partner agencies [*Canada Border Services Act*, s. 5].

The CBSA is the first line of defence in preventing inadmissible foreign nationals and/or goods from entering Canada, as well as managing the export of goods that may be prohibited, controlled or regulated. In this role, the CBSA works with Immigration, Refugees and Citizenship Canada (IRCC), the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) to protect Canada’s security at the border.

The Agency also collects, analyses, produces and disseminates intelligence to its national security partners across the Government of Canada. As such, the CBSA requires timely, accurate and actionable information in order to support its own operations, and to assist its Government of Canada partners [*Canada Border Services Act*, s. 13 (2)].

Responsibilities:

**Intelligence Gathering and Dissemination:** The CBSA conducts intelligence activities (focus on threats that pose the highest risk and consider the broader enforcement continuum) and provides support to a wide range of CBSA programs as well as external stakeholders.

**Risk Assessment and Targeting:** The CBSA conducts risk assessments of persons and shipments prior to their arrival, and those that have been identified as potential threats to the safety and security of Canada are then “targeted” for further examination upon their arrival.

**Marine Security Operations:** The CBSA works with other government of Canada partners and shares intelligence, surveillance and reconnaissance information related to the marine mode of travel in addition to facilitating organized responses to national security and other threats.

**Document Integrity:** The CBSA seizes fraudulent travel and identity documents to prevent further improper use of these documents. The fraudulent use of travel and identity documents is often associated with activities, which may pose a risk to national security, such as international smuggling of migrants, trafficking in persons, terrorist mobility, espionage, and the smuggling of drugs, weapons and other illicit goods.

**Inland Enforcement:** The CBSA conducts inland enforcement activities, which contribute directly to national security outcomes. These activities include immigration investigations, detentions, and hearings, criminal investigations and removals of inadmissible foreign nationals.

**Ports of Entry:** CBSA officers at ports of entry are Canada’s first point of contact in the examination and questioning of travelers entering Canada. CBSA officers have the authority to examine and search travelers for suspected customs or immigration-related violations, and to seize fraudulent or invalid travel documents. In this way, the CBSA also collects intelligence that supports national security investigations [*Immigration and Refugee Protection Act*, s. 3].

**Security Screening:** The CBSA conducts the evaluation of temporary and permanent resident applicants, and refugee claimants for involvement in: espionage, subversion, and terrorism; human or international rights violations; and, organized criminality. The CBSA makes recommendations to IRCC with respect to a foreign national’s admissibility to Canada on security grounds [*Immigration and Refugee Protection Act*, s. 34 (1), 35 & 37].

**Lookout Issuance:** The CBSA issues lookouts and develop intelligence products that identify a person, corporation, conveyance or shipment that may pose a threat to the health, safety,

economy, environment or national security of Canada. Subjects of concern are handled appropriately once they reach the Canadian Border [*Customs Act*, s. 11 – 13].

Export Control: The CBSA works with various other government departments to control the export of prohibited, controlled or regulated goods from Canada to countries that may pose a threat to the national security of Canada or its allies [*Customs Act*, s. 19 (1)].

## Canada Revenue Agency

The Canada Revenue Agency (CRA) acts as the Government of Canada's responsible authority for preventing, detecting, and responding to the exploitation of charitable resources to support terrorism. The *Income Tax Act* (ITA) provides the CRA with a legal framework to support the regulation of Canada's charitable sector. The *Charities Registration (Security Information) Act* (CRSIA) demonstrates Canada's commitment to participating in concerted international efforts to deny support to those who engage in terrorist activities, to protect the integrity of the registration system for charities under the ITA, and to maintain the confidence of Canadian taxpayers that the benefits of charitable registration are made available only to organizations that operate exclusively for charitable purposes [CRSIA, s. 2 (1)].

A specialized centre of expertise within the CRA's Charities Directorate is responsible for working to prevent the abuse of Canada's charitable sector to support terrorism. The Charities Directorate is mandated to prevent organizations with ties to terrorism from obtaining charitable registration in Canada, and to detect and address the exploitation of already registered Canadian charities to support terrorism. This is accomplished via a registration review function, monitoring and audit programs, and through education.

The Charities Directorate utilizes an intelligence-led, risk-based investigative process to identify applicants and registered charities that may pose a risk to the integrity of the charities registration system under the ITA because of ties to terrorist groups. This process may include information sharing with national security partners.

In exceptional circumstances, the CRSIA's security certificate process – Certificate Based on Intelligence – allows for the reliance on information that, if disclosed, could be injurious to national security, when determining eligibility to obtain or maintain charitable registration in Canada [CRSIA, s. 4 (1)].

In carrying out the CRA's national security mandate, the Charities Directorate protects the integrity of the charitable registration system and contributes to a whole-of-government approach to combatting terrorism.

## Canadian Food Inspection Agency

The Canadian Food Inspection Agency (CFIA) plays an important role in the federal government's capacity to respond rapidly and effectively in the event of a food safety emergency or a threat to agricultural or forest biosecurity, including bioterrorism or agro-terrorism (terrorism directed towards Canada's agricultural resource base). The CFIA is dedicated to safeguarding food, animals and plants, which enhances the health and well-being of Canada's people, environment and economy. To this end, CFIA's surveillance, detection and inspection programs are designed to detect the presence of hazards (such as contaminants, disease or pests) in food, animals and plants and their products, and provide early warning of risks arising from the presence of these hazards, whether they are introduced accidentally or intentionally.

The CFIA does this through the administration and enforcement of a number of Acts including the *Feeds Act*, *Fertilizers Act*, *Health of Animals Act*, *Plant Protection Act*, *Safe Food for Canadians Act* and the *Seeds Act* [*Canadian Food Inspection Agency Act*, s. 11 (1)]. Where the Minister believes that there is a product that poses a risk to public, animal or plant health, the product can be recalled [*Canadian Food Inspection Agency Act*, s. 19 (1)].

In addition, the CFIA enforces the *Food and Drugs Act* as it relates to food and administers the provisions of the *Food and Drugs Act* as they relate to food, except for provisions that relate to public health, safety or nutrition [*Canadian Food Inspection Agency Act*, s. 11 (3)].

## Canadian Nuclear Safety Commission

The Canadian Nuclear Safety Commission (CNSC) has the mandate to regulate nuclear activities, in order to protect the health, safety and security of Canadians and the environment, and to implement Canada's international commitments on the peaceful use of nuclear energy under the authority of the *Nuclear Safety and Control Act* (NSCA).

The CNSC is mandated to prevent the unreasonable risk to national security associated with the development, production and use of nuclear energy, and production, possession and use of nuclear substances, prescribed equipment and prescribed information [NSCA, s. 3 (a)].

The CNSC is responsible for the implementation of Canada's international obligations related to respecting the control of the development, production and use of nuclear energy, including the non-proliferation of nuclear weapons and nuclear explosive devices [NSCA, s. 3 (b)].

The objects of the CNSC include the regulation of the development, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment and prescribed information in order to prevent unreasonable risk to national security associated with that development, production, possession or use [NSCA, s. 9].

The CNSC regulates the nuclear industry in order to protect Canadians against sabotage, terrorism, interference with critical infrastructure and cybersecurity, activities that undermine the security of Canada, as well as measures to control the non-proliferation of nuclear weapons and nuclear explosive devices. The CNSC is provided with various powers to regulate national security in relation to the nuclear industry.

Responsibilities:

**Licensing:** The CNSC has the authority to issue licences for nuclear related activities, by which the CNSC imposes those measures it considers necessary to the maintenance of national security and measures required to implement international obligations to which Canada has agreed [NSCA, s. 24 (4)].

The *Nuclear Safety and Control Act* (NSCA) prohibits the import and export of a nuclear substance, prescribed equipment or prescribed information without a licence issued under the NSCA, subject to applicable regulations [s. 26 (a)]. Regulations, such as the General Nuclear Safety and Control Regulations and the Nuclear Non-Proliferation Import and Export Control Regulations establish requirements on applicants. Implementation of export and import controls under the CNSC's responsibility responds directly to risks of proliferation of nuclear weapons and nuclear explosive devices.

**Inspection:** The CNSC, through inspectors, can order a licensee to take any measure the inspector considers necessary to maintain national security or compliance with international obligations to which Canada has agreed [NSCA, s. 35 (1)].

**Regulation-Making:** The CNSC has the responsibility to regulate the nuclear industry within Canada. This is to be considered for all nuclear-related activities and at all stages of a nuclear facility's lifecycle [NSCA, s. 44 (1)].

The CNSC has the statutory power to make regulations to ensure the maintenance of national security and compliance with Canada's international obligations in the development, production and use of nuclear energy and the production, use, possession, packaging, transport, storage and disposal of nuclear substances, prescribed equipment and prescribed information [s. 44 (1) (m)].

**Exceptional Powers:** The CNSC has the power, in case of emergency, to make an order that it considers necessary to maintain national security and compliance with Canada’s international obligations [NSCA, s. 47 (1)].

## Canadian Security Intelligence Service

The Canadian Security Intelligence Service’s (CSIS) core mandate is to investigate activities that may on reasonable grounds be suspected of constituting threats against Canada. Threats to the security of Canada are defined and encompass terrorism (or more precisely “acts of serious violence... for the purpose of achieving a political, religious or ideological objective”), espionage and sabotage, foreign-influenced activities that are clandestine, deceptive, or threaten a person, as well as domestic subversion aimed at the overthrow by violence of the constitutional order of government. Lawful advocacy, protest and dissent are excluded, unless carried out in conjunction with any of the activities referred to above [*Canadian Security Intelligence Service Act*, s. 2].

To this end, CSIS collects, analyzes and retains intelligence to the extent that it is strictly necessary to do so, and reports to and advises the Government of Canada (GOC). The Service may perform its duties within or outside Canada [*Canadian Security Intelligence Service Act*, s. 12]. CSIS may take measures to reduce threats if there are reasonable grounds to believe the activity constitutes a threat to the security of Canada [Canadian Security Intelligence Service Act, s. 12.1].

CSIS may provide security assessments to GOC departments [*Canadian Security Intelligence Service Act*, s.13]. With the approval of the Minister, CSIS may also enter into an arrangement to provide security assessments to the government of a province or a department thereof, or any police force in a province. Security assessments are defined in the CSIS Act as an “appraisal of the loyalty to Canada and, so far as it relates thereto, the reliability of an individual.” For example, an assessment of loyalty under section 13 would include consideration of whether an individual is or may engage in activities that undermine the security of Canada, such as interfering with GOC capabilities in relation to intelligence, defense, border, operations, diplomatic or consular relations, economic or financial stability, etc.

The provision of assessments supports the detection, investigation, analysis and prevention of activities that undermine the sovereignty and security of Canada, as well as the security of the people of Canada. In support of this mandate, CSIS administers the Government Security Screening Program (as described below). CSIS may provide any minister of the Crown with

information relating to security matters or criminal activities, that is relevant to the exercise of any power or the performance of any duty or function by that Minister under the *Citizenship Act* or the *Immigration and Refugee Protection Act*. In support of this mandate, CSIS administers the Immigration Security Screening Program (as described below).

The objective is to support programs aimed at preventing non-Canadians (e.g., temporary resident applicants, prospective permanent residents or prospective citizens) who pose a threat to the security of Canada from entering or receiving status in Canada. CSIS security advice is provided to the Canada Border Services Agency (CBSA) and Immigration, Refugees and Citizenship Canada (IRCC) [Canadian Security Intelligence Service Act, s. 14], and in turn, these partners make the decision regarding a person's admissibility into Canada. CSIS may conduct investigations for the purpose of providing security assessments pursuant to section 13 and providing advice pursuant to section 14 [Canadian Security Intelligence Service Act, s. 15].

Responsibilities:

**Intelligence Program:** The Intelligence Program is one of CSIS' key business lines.

- **Security Intelligence** encompasses the collection, analysis, retention and reporting of intelligence in regard to activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and the safety of Canadians [Canadian Security Intelligence Service Act, s. 12]. Under this sub-program, CSIS' role is to investigate threats, collect and analyze intelligence that is then used to report to and advise the GOC, so as to protect the country and its citizens. CSIS collects information in Canada and abroad through regional offices and foreign posts. In addition to open sources of information and extensive cooperation and liaison with domestic and foreign partners, CSIS collects information through a variety of techniques including human sources and a range of warranted and non-warranted techniques, including physical surveillance, and warranted interception of communications. CSIS analysts assess the quality of information gathered, and convert the information into useful security intelligence that is shared nationally and internationally under strict compliance with Ministerial Direction (MD) and operational policies.

**Security Screening Program:** The Security Screening program is one of the main responsibilities of CSIS and among its most visible functions. The Security Screening program has two key sub-programs: Government Security Screening and Immigration Security Screening.



- The Government Security Screening (GSS) sub-program, as mandated by sections 13 and 15 of the CSIS Act, provides security assessments on individuals whose employment with the GOC (with exception of the Royal Canadian Mounted Police (RCMP)), provincial governments and other organizations requires them to have access to classified information or sensitive sites (for example, ports, nuclear facilities, airports, or the Parliamentary precinct). In addition to conducting the screening required for these security and site access clearances, the GSS sub-program assists the RCMP with the accreditation process for persons seeking access or participating in major events in Canada; and provides, under reciprocal screening agreements, security assessments to foreign governments, agencies and international organizations on Canadians seeking to reside and work in another country. Client departments and agencies are exclusively responsible for decisions regarding the granting, denial or revocation of security clearances, which is informed by security assessments provided by CSIS.
- The Immigration Security Screening (ISS) sub-program, under the *Immigration and Refugee Protection Act and the Citizenship Act* and sections 14 and 15 of the CSIS Act, provides security advice to the CBSA and IRCC on persons attempting to travel to or claim status in Canada who may represent a threat to national security. Important components of the ISS sub-program include visitor visa vetting, the front-end screening of refugees, and the screening of permanent resident and citizenship applications. CBSA and IRCC retain responsibility for final decisions regarding these applications.

**Review of Foreign Investments:** CSIS also supports the review of investments by non-Canadians in Canada under the *Investment Canada Act* National Security Review, as a prescribed investigative body [s. 7].

## Communications Security Establishment

The Communications Security Establishment (CSE) is the national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance [*Communications Security Establishment Act*, s. 15(1)].

CSE's mandate has five aspects: foreign intelligence, cybersecurity and information assurance, defensive cyber operations, active cyber operations and technical and operational assistance [*Communications Security Establishment Act*, s. 15(2)].



## Foreign Intelligence

Under the Foreign Intelligence aspect of its mandate, CSE acquires information from or through the global information infrastructure (GII) and analyses, uses, and disseminates the information for the purpose of providing foreign intelligence, in accordance with the government of Canada's intelligence priorities [*Communications Security Establishment Act*, s. 16].

CSE's foreign signals intelligence operations are clearly and carefully targeted, by law, at the activities of foreign individuals, states, and organizations or terrorist groups that have implications for Canada's international affairs, defence or security.

The ACT includes the following constraints on CSE's foreign intelligence mandate:

- Explicit statutory prohibition on directing activities at Canadians or any person in Canada;
- Explicit statutory requirement to protect the privacy of Canadians and persons in Canada; and
- Ministerial Authorization regime that applies to all of CSE's acquisition of information from the GII where the activity to acquire it would otherwise be contravening any other Act of Parliament or interfere with the reasonable expectation of privacy of a Canadian or person in Canada.

## Cybersecurity and Information Assurance

Under the Cybersecurity and Information Assurance aspect of its mandate, CSE:

Provides advice, guidance, and services to help ensure the protection of:

- Federal institutions' electronic information and information infrastructures; and
- Electronic information and information infrastructures designated by the Minister of National Defence as being of importance to the Government of Canada.

Acquires information from the GII and other sources in order to provide such advice, guidance, and services [*Communications Security Establishment Act*, s. 17].

The Act implements the following constraints on CSE's cyber security and information assurance mandate:

- Explicit statutory prohibition on directing activities at Canadians or any person in Canada;
- Explicit statutory requirement to protect the privacy of Canadians and persons in Canada; and
- Ministerial Authorization regime that applies to all of CSE's acquisition of information from the GII where the activity to acquire it would otherwise be contravening any other Act of Parliament or interfere with the reasonable expectation of privacy of a Canadian or person in Canada.

CSE also carries out activities on information infrastructures to identify or isolate malicious software, prevent malicious software from harming those information infrastructures or mitigate any harm that malicious software causes to them, and analyze information in order to be able to provide advice on the integrity of supply chains and on the trustworthiness of telecommunications, equipment and services [*Communications Security Establishment Act*, s. 23(3)].

### Assistance to Federal Security & Intelligence Partners

Under the Assistance to Federal Security & Intelligence Partners aspect of its mandate, CSE provides technical and operation assistance to federal law enforcement and security agencies, the Canadian Armed Forces, and the Department of National Defence in their performance of their lawful duties [*Communications Security Establishment Act*, s. 20].

CSE has the same authority to carry out an activity as the agency requesting the assistance. CSE is also to be subject to any restrictions or conditions placed on the agency requesting that assistance, such as a warrant or applicable law.

CSE has strict internal monitoring of assistance mandate activities for legal and policy compliance.

### Foreign Cyber Operations

Under the defensive cyber operation of its mandate, CSE takes action on or through the GII to help protect:

- Federal institutions' electronic information and information infrastructures; and

- Electronic information and information infrastructures designated by the Minister of National Defence as being of importance to the government of Canada [*Communications Security Establishment Act*, s. 18].

Under the active cyber operation aspect of its mandate, CSE carries out activities on or through the GII to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to Canada's defence, security or international affairs [*Communications Security Establishment Act*, s. 19].

CSE is prohibited from directing defensive and active cyber operations activities at Canadians, any person in Canada, or the GII in Canada. The Act requires that these activities be reasonable and proportional, and prohibits CSE from causing death or bodily harm, or willfully attempting to obstruct, pervert or defeat the course of justice or democracy.

#### Investment Canada Act

CSE analyses information for the purpose of providing advice with regard to investments injurious to National Security [*Communications Security Establishment Act*, s. 23(2)].

#### Other Activities

Additionally, CSE carries out the following activities in furtherance of its mandate:

- Acquiring, using, analyzing, retaining or disclosing publicly available information;
- Acquiring, using, analyzing, retaining or disclosing infrastructure information for the purpose of research and development, for the purpose of testing systems or conducting cybersecurity and information assurance activities on the infrastructure from which the information was acquired; and

Testing or evaluating products, software and systems, including testing or evaluating them for vulnerabilities [*Communications Security Establishment Act*, s. 23(1)].

## Department of Immigration, Refugees and Citizenship Canada (Department of Citizenship and Immigration)

The Department of Citizenship and Immigration Canada, hereafter referred to as Immigration, Refugees and Citizenship Canada (IRCC), is responsible for all matters over which Parliament has jurisdiction relating to citizenship and immigration, and that are not by law assigned to any other department, board or agency of the Government of Canada [Department of Citizenship and Immigration Act, s. 4].

IRCC's responsibilities include facilitating the arrival and integration of migrants into Canada, protecting the health, safety and security of Canadians, and determining the admissibility of individuals to Canada, as well as managing the citizenship program. The Minister of IRCC is responsible for issuance of Canadian passports and travel documents.

These mandates and responsibilities place IRCC as a critical link in the Government of Canada's national security regime. IRCC's support for national security priorities focuses on ensuring the integrity of the citizenship, immigration, refugee and passport processes and programs.

IRCC works closely with its security and enforcement partners to proactively identify applicants who are inadmissible to Canada due to security concerns, to prohibit the acquisition of citizenship status by those who engage in activities deemed to undermine Canada's national security, and to implement cancellation, refusal and revocation decisions rendered by the Minister of Public Safety and Emergency Preparedness on the passports of persons posing a threat to national security.

### Responsibilities:

**Passport Services:** IRCC conducts entitlement reviews and may launch an administrative investigation to collect further information to determine a subject's eligibility to passport services [Canadian Passport Order, s. 9 – 11.4].

The Minister of Public Safety and Emergency Preparedness has the authority to cancel, refuse (including authority to refuse passport services for up to 10 years) or revoke the passport of individuals of concern to national security and communicate these decisions to IRCC to take the required action.

**Immigration and Inadmissibility:** In collaboration with its security and enforcement partners, IRCC ensures that individuals who are determined to be inadmissible for criminality,

organized criminality, human or international rights violations, security, misrepresentation and other grounds defined in Part 1, Division 4 of the *Immigration and Refugee Protection Act* (IRPA) are not permitted to enter or remain in Canada [IRPA, s. 34 – 42].

IRCC processes pre-removal risk assessment applications, which may include those submitted by persons who are inadmissible on grounds of security, violating human or international rights, organized criminality or serious criminality. In some cases, this involves an assessment of whether the applicant is a danger to the public in Canada or a danger to the security of Canada [IRPA, s. 77 (1) & 112 (1)].

IRCC conducts assessments and issues ministerial opinions on whether protected persons who have been found to be inadmissible for security reasons, human rights violations, serious criminality, or organized crime represent a danger to the public in Canada or danger to the security of Canada [IRPA, s. 115 (1) & (2)].

**Revocations of Citizenship:** IRCC is responsible for conducting revocations of citizenship. More specifically, the *Citizenship Act* provides that a person's citizenship, or renunciation of citizenship, may be revoked if the person obtains, retains, renounces, or resumes citizenship by false representation, fraud or knowingly concealing material circumstances.

Examples of fraud or misrepresentation can include, but are not limited to, the use of a false identity, failure to disclose criminal convictions prior to obtaining citizenship, and by making false statements to obtain citizenship [*Citizenship Act*, s. 10 & 10.1].

IRCC may make a report to the National Security and Intelligence Review Agency (NSIRA) for individuals who should not be granted citizenship, administered the oath of citizenship or be issued a certificate of renunciation for reasons that they have engaged, are engaged, or will engage in activities that constitute a threat to the security of Canada [*Citizenship Act*, s. 19].

## Department of Finance

The *Financial Administration Act* establishes the Department of Finance and sets out the role of the Minister of Finance. The Minister of Finance is responsible for the supervision, control and direction of all matters relating to the financial affairs of Canada not by law assigned to the Treasury Board or to any other minister [*Financial Administration Act*, s. 14 & 15].

Responsibilities:

**Money Laundering and Terrorist Financing:** The Department of Finance is responsible for Canada's anti-money laundering and anti-terrorist financing (AML/ATF) regime and develops anti-money laundering and anti-terrorist financing policy, including with respect to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and its regulations. This includes the assessment of information and intelligence about threat actors, both domestic and foreign, and how these actors exploit vulnerabilities to launder money and finance terrorism [PCMLTFA, Part 1.1].

**Financial Sector Stability and Cyber Security:** The Department of Finance has oversight responsibility for the stability of the financial sector, including threats to financial stability deriving from operational risks, such as physical and cyber security threats. Finance's policy and operational responsibilities related to the prudential regulation of the financial sector help to ensure that the security and integrity of Canada's financial sector is maintained, in order to avoid activities and occurrences that could otherwise destabilize Canada's economy or key members of the financial sector. Finance works to ensure that cyber and security threats are mitigated and that the financial sector is well protected against risks and vulnerabilities.

**Financial Institution Transactions Approvals:** The Minister of Finance has authorities to approve material changes to a financial institution's lifecycle, such as incorporations or changes in ownership. When considering whether to grant, deny, revoke, or amend an approval, the Minister may take into account a broad set of factors, including national security considerations. Authorities are set out in statutes that accord to the type of financial institution, i.e., for banks (Bank Act), trust and loan companies (Trust and Loan Companies Act) or insurance companies (Insurance Companies Act).

**Stability of the Global Economic and Financial System:** The Minister of Finance is mandated with responding to economic risks to Canada from global or regional economic instability, representing Canada at the Group of Seven (G7) and Group of 20 (G20) Finance Ministers' process and is legislated to oversee Canada's participation in the International Monetary Fund, World Bank, and European Bank for Reconstruction and Development. The Department also has core responsibility for Canada's engagement with the Organisation for Economic Co-operation and Development, World Trade Organization, and regional development banks, such as the Asian Development Bank, African Development Bank, Caribbean Development Bank, and Inter-American Development Bank. All of these institutions and groups are tasked with taking actions that can impact global or regional economic and financial stability, with potential spillovers to stability in Canada.

## Global Affairs Canada (Department of Foreign Affairs)

The Department of Foreign Affairs, Trade and Development (styled as Global Affairs Canada) manages Canada's diplomatic and consular relations with foreign governments and international organizations, engaging and influencing international players to advance Canada's political, economic and development interests and the values of freedom, democracy, human rights and the rule of law [Department of Foreign Affairs, *Trade and Development Act*, s. 10].

Responsibilities:

**Membership in International Defence and Security Organizations:** Global Affairs Canada manages the country's membership in organizations such as the United Nations, the North Atlantic Treaty Organization, the North American Aerospace Defence Command, the Organization of American States, the Group of Seven (G7), the Conference on Disarmament, and the Organization for Security and Cooperation in Europe. These organizations deal with traditional threats to security as well as terrorism, defending our democracy from threats from foreign state and non-state actors, and threats to cybersecurity and space security.

**Security-Focused Diplomatic Reporting:** Under the Global Security Reporting Program, Global Affairs Canada generates focused diplomatic reporting on security and stability issues in countries of strategic interest to Canada.

**Security-Related Incidents Outside of Canada:** Global Affairs Canada leads Canada's response to national security-related hostage-takings abroad through a coordinated effort drawing on the special skills of the federal national security community. Global Affairs Canada missions and diplomats also play an important role when Canadian citizens are imprisoned or accused of terrorist activity abroad. Global Affairs Canada also coordinates Canadian responses to crises and natural disasters abroad, which may involve national security interests.

**International Security Programming:** Global Affairs Canada supports policies and delivers programs that strengthen the capacity of international partners to support stabilization, anti-crime, counter-terrorism, and reduction of weapons and materials of mass destruction.

**Maintenance of an International Network of Missions:** This network serves as a platform for Global Affairs Canada, and other institutions that benefit from the department's resources abroad, to fulfill its mandate. Management of the platform includes assessment of threats to the security of missions abroad; provision of appropriate protection; and, management of any residual risks to life and property, including diplomatic personnel and assets abroad.

**Multilateral Counter-Proliferation:** These efforts relate to preventing the transit of weapons of mass destruction (WMD) and related materials among states and non-state actors of proliferation concern. These efforts include the Proliferation Security Initiative focused on the interdiction of WMD proliferation and United Nations Security Council Resolution (UNSCR) 1540, aimed at preventing the terrorist acquisition of WMD and related materials. Each of these initiatives call on States to take steps to enhance national legal authority to strengthen key counter-proliferation measures, including the rapid exchange of relevant information concerning suspected proliferation activity.

**Listing of Terrorist Entities:** Global Affairs Canada plays a key role in the listing of terrorist entities under the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism and the United Nations Al-Qaida and Taliban Regulations.

**Administration of the *United Nations Act*:** This Act establishes the authority for the implementation of United Nations Security Council resolutions under article 41 of the United Nations Charter.

**Management of the *Chemical Weapons Convention Implementation Act*:** Global Affairs Canada gathers information relevant to the production, processing, consumption, import and export of certain chemicals and related facilities in its management of the *Chemical Weapons Convention Implementation Act*.

Administration of the *Export and Import Permits Act*, the *Special Economic Measures Act*, and the *Remote Sensing Space Systems Act*: Global Affairs Canada administers the *Export and Import Permits Act*, the *Special Economic Measures Act*, and the *Remote Sensing Space Systems Act*, each of which regulates the export or import of goods, services or technology, in part to protect the national security of Canada and its allies.

**Authority Delegated by the *Canadian Security Intelligence Service (CSIS) Act*:** The Minister of Foreign Affairs plays a formal role under the *CSIS Act*:

- Under section 16, the Minister of Foreign Affairs may request CSIS assistance in the collection of information or intelligence; and,



- Under section 17, the Minister of Foreign Affairs is consulted prior to CSIS seeking approval to enter into arrangements with foreign states, international organizations of states, or institutions thereof.

## Department of Health

Health Canada (HC) is responsible for all matters over which Parliament has jurisdiction relating to the promotion and preservation of the health of the people of Canada not by law assigned to any other department, board or agency of the Government of Canada [*Department of Health Act*, s. 4 (1)].

HC's powers, duties and functions relating to health include the promotion and preservation of the physical, mental and social well-being of the people of Canada and the protection of the people of Canada against risks to health and the spreading of diseases [*Department of Health Act*, s. 4 (2)].

Responsibilities:

**Health-Related Emergencies:** HC is responsible to identify the risks that are within or related to its area of responsibility, and to prepare emergency management plans in respect of those risks; maintain, test and implement those plans; and conduct exercises and training in relation to those plans [*Emergency Management Act*, s. 6 (1)].

**Nuclear Emergencies:** Through the Federal Nuclear Emergency Plan, HC is responsible for the planning and implementation of emergency measures to protect the safety and security of Canadians in the event of a nuclear emergency (outside of the site boundary of a nuclear facility).

**Counter-Terrorism:** HC provides radiological surveillance support to the Royal Canadian Mounted Police's (RCMP) chemical, biological, radiological and nuclear (CBRN) National Team during major public events and coordinates the federal response to a major emergency involving radiological or nuclear materials under the Federal Terrorism Response Plan and Federal Nuclear Emergency Plan.

**Nuclear Non-Proliferation:** To fulfil Canada's obligations under the Comprehensive Nuclear Test Ban Treaty, including verification activities, HC operates and maintains facilities and laboratories to perform analyses of samples and data from radionuclide monitoring stations.

## Department of National Defence / Canadian Armed Forces

The Crown Prerogative, in relation to National Defence, is the primary enabling authority under which the Department of National Defence and the Canadian Armed Forces (DND/CAF) conducts its operations and activities. In the area of National Defence activities, the Crown Prerogative is regularly exercised through a variety of mechanisms, including the promulgation of Orders-in-Council relating to defence activities within Canada and abroad, the issuance of Cabinet direction to the CAF through the Minister of National Defence and the Chief of Defence Staff, and the development of agreements and arrangements with foreign and domestic partners.

The *National Defence Act* (NDA) is the enabling legislation for the DND/CAF, but it does not set out a specific national security mandate for the DND and CAF. That being said, the NDA provides statutory authority for the CAF to:

- Provide assistance in respect of law enforcement [s. 273.6 (2)]
- Provide aid to the civil power where there is a riot or disturbance of the peace beyond the powers of the civil authorities to suppress [s. 274 – 285]
- Perform any duty involving public service [s. 273.6 (1)]

The responsibilities of the DND/CAF are primarily assigned through an exercise of the Crown prerogative. However, Canada's Defence Policy, Strong, Secure, Engaged, provides Government direction to the DND/CAF on its missions, responsibilities and the expected concurrency of operations. At any given time, the Government of Canada can exercise the Crown Prerogative to call upon the CAF to undertake these missions, which include:

- Detect, deter, and defend against threats to or attacks on Canada;
- Detect, deter, and defend against threats to or attacks on North America in partnership with the United States, including through NORAD;
- Lead/contribute forces to NATO and coalition efforts to deter and defeat adversaries, including terrorists to support global stability;
- Lead/contribute to international peace operations and stabilization missions with the United Nations, NATO, and other multilateral partners;
- Engage in capacity building to support the security of other nations and their ability to contribute to security abroad;
- Provide assistance to civil authorities and law enforcement, including counter-terrorism, in support of national security and security of Canadians abroad;

- Provide assistance to civil authorities and non-governmental partners in responding to international and domestic disasters or major emergencies; and,
- Conduct search and rescue operations.

## Department of Public Safety and Emergency Preparedness

Public Safety (PS) is responsible for all matters that have not been assigned by law to another department, board, or agency of the Government of Canada relating to public safety and emergency management, as specified under its enabling Act, the *Department of Public Safety and Emergency Preparedness Act* (DPSEPA) [s. 4 (1)].

PS is responsible for exercising leadership, at the national level, for all matters relating to public safety and emergency preparedness [DPSEPA, s. 4 (2)].

PS coordinates the activities of the entities for which the Minister is responsible, including the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS) and the Canada Border Services Agency (CBSA). PS also establishes strategic priorities for activities relating to public safety and emergency preparedness [DPSEPA, s. 5].

PS plays a leadership role in facilitating the sharing of information, where authorized, to promote public safety objectives. PS coordinates, initiates, implements, and promotes policies, programs, activities, and projects related to national security, public safety, and emergency preparedness [DPSEPA, s. 6 (1)].

### Responsibilities:

**Counter-Proliferation:** PS promotes a coordinated approach across government on counter-proliferation policy aimed at preventing state and non-state actors from engaging in proliferation activities through the detection, denial, and rapid response to activities relating to proliferation both in Canada and abroad.

**Counter-Radicalization:** Within PS, the Canada Centre for Community Engagement and Prevention of Violence works alongside government, non-government, and community-based partners to provide a leadership role on Canada's efforts to prevent radicalization to violence.

**Counter-Terrorism:** Through the Federal Terrorism Response Plan, PS is responsible for coordinating responses to domestic terrorist incidents by:

- establishing a notification and information sharing protocol;

- setting out information sharing processes for security and intelligence agencies to use in the event of a terrorist incident;
- identifying the communications framework for the Government of Canada to use in the event of a terrorist incident;
- ensuring that linkages exist between the immediate security and intelligence response, as well as elements of crisis response and consequence management.

**Critical Infrastructure:** Through the National Strategy and Action Plan for Critical Infrastructure, PS (in collaboration with multiple federal-provincial-territorial and private sector partners) works to enhance the resiliency of Canada’s vital assets and systems, such as our food supply, electricity grids, transportation, communications, and public safety systems.

**Cyber Security:** Through the National Cyber Security Strategy (NCSS), PS works to protect citizens, businesses, and government partners from cyber threats that continue to evolve in a world with ever-changing technological capabilities. PS coordinates the implementation of the NCSS, promotes collaboration and innovation in cyber security amongst local and foreign governments with the private sector, academia, and other partners for the achievement of a secure and prosperous Canada in the digital age.

**Hostage-Taking:** PS supports Global Affairs Canada in the management of hostage-taking cases of Canadians abroad, including in initiation, coordination, and implementation of policies. PS is also engaged on plans or proposals that are developed as they relate to partner agencies within the Public Safety portfolio.

**Hostile State Activity:** PS leads on horizontal policy and coordination to counter hostile state activity, and supports specific initiatives led by other government departments in this respect. PS engages with domestic and international partners, including as a supporting partner to Global Affairs Canada, the leader of the G7 Rapid Response Mechanism.

**Relevant Lawful Authorities** (Please contact department for further clarification):

**Aviation** *Aeronautics Act, Canadian Aviation Security Regulations, 2012 and aviation security measures enacted pursuant to s. 4.72 of the Aeronautics Act; Canadian Air Transport Security Authority Act; Preclearance Act, 2016; Secure Air Travel Act and Secure Air Travel Regulations.*

**Marine** *Marine Transportation Security Act and Marine Transportation Security Regulations; Canada Marine Act.*

**Rail / Surface** *Railway Safety Act; International Bridges and Tunnels Act; Transportation of Dangerous Goods by Rail Security Regulations.*

**Multi-Modal** *Railway Safety Act; International Bridges and Tunnels Act; Transportation of Dangerous Goods by Rail Security Regulations.*

**Migrant Smuggling:** PS is engaged in developing and implementing policies, programs, and legislative initiatives related to migrant smuggling with a national security nexus. PS is also engaged in whole-of-government operational responses under Canada’s Migrant Smuggling Prevention Strategy.

**Emergency Management:** Housed at PS, the Government Operations Centre (GOC) leads and supports an all-hazards integrated federal emergency response to events (potential or actual, natural or human-induced, accidental or intentional) of national interest.

The GOC provides 24/7 monitoring and reporting, national-level situational awareness, prepares and distributes warning products and integrated risk assessments, as well as national-level planning and whole-of-government response management. During periods of heightened response, the GOC is augmented by staff from other government departments and agencies and non-governmental organizations who work in the GOC physically and connect to it virtually [Emergency Management Act, s. 3, 4 (1) & 6 (1)].

**Passport Issues:** PS provides advice in certain circumstances when:

- a passport is not to be issued or is to be revoked when there are reasonable grounds to believe that the decision is necessary to prevent the commission of a terrorism offence, as defined in section 2 of the Criminal Code, or for the national security of Canada or a foreign country or state [Canadian Passport Order, s. 10.1].

- a passport is to be cancelled if there are reasonable grounds to suspect that the decision is necessary to prevent the commission of a terrorism offence, as defined in section 2 of the Criminal Code, or for the national security of Canada or a foreign country or state [Canadian Passport Order, s. 11.1 (2)].
- a passport has been cancelled under section 11.1, and the holder wishes to apply to the Minister of Public Safety and Emergency Preparedness to have the cancellation reconsidered [Canadian Passport Order, s. 11.3 (1)].

**Review of Foreign Investments:** PS leads and coordinates the review process to identify any national security concerns posed by investments by non-Canadians in Canada. The provisions within the *Investment Canada Act* provide a robust framework for reviewing foreign investments for various reasons, such as to protect defense capabilities, safeguard against the transfer of sensitive technologies, and ensure no potential involvement related to organized crime [*Investment Canada Act*, PART IV.1].

**CSIS Arrangements:** The Director of CSIS is accountable to the Minister of Public Safety and Emergency Preparedness. As such, the Service, with the approval of the Minister, may:

- enter into an arrangement with any Government of Canada department; the government of a province, its departments, and police force; the government of a foreign state; and an international organization for the purpose of performing its duties and functions under the CSIS Act [s. 17].
- make an application to a judge for a warrant or the renewal of a warrant to enable the Service to investigate a threat to the security of Canada [CSIS Act, s. 21]; and,
- make an application to a judge for a warrant or the renewal of a warrant to take measures, within or outside Canada, to reduce a threat to the security of Canada [CSIS Act, s. 22].

**Listing of Terrorist Entities:** PS is responsible for making recommendations on the listing of individuals and groups that meet the legal threshold to be designated as terrorist entities under the Criminal Code [s. 83.05].

**Security Certificates:** PS, in partnership with Immigration, Refugees and Citizenship Canada, is responsible for authorizing the issuance of a security certificate, an immigration proceeding for the purpose of removing from Canada non-Canadians who are inadmissible for reasons of national security, violating human or international rights, or involvement in organized or serious crimes [Immigration and Refugee Protection Act, s. 77 (1)].

**Passenger Protect Program:** PS, in partnership with Transport Canada, administers the Passenger Protect Program, which screens commercial flights to, from, and within Canada in an attempt to prevent transportation security threats (injurious activity aboard flights) and to prevent individuals from attempting to travel abroad to commit certain terrorism offences, such as terrorist attacks, funding for weapons, training, and recruitment [Secure Air Travel Act, s. 8 (1)].

PS oversees the administrative recourse function of the Passenger Protect Program, which allows a listed person who has been denied transportation as a result of a direction made under section 9 of the SATA to apply to the Minister to have their name removed from the list [Secure Air Travel Act, s. 15 (1)].

**Charities Certificates:** PS, in conjunction with the CRA, may authorize the issuance of a certificate that aims to prevent the abuse of Canada's charitable sector by those seeking to directly or indirectly allocate resources to an entity that is a listed entity under s. 83.01 (1) of the Criminal Code. These entities may include, but are not limited to, those that support or engage in activities related to terrorism [Charities Registration Security Information Act, s. 4 (1)].

## Department of Transport

Transport Canada (TC) supports Canada's national security and intelligence community in fulfilling its broader departmental mandate to ensure a safe, secure, and efficient transportation system. Much of TC's security mandate involves preventing and mitigating risks associated with unlawful interference in the Canadian transportation system.

In the event that a national security threat or incident affecting the transportation system (all modes) should occur, TC is responsible for supporting core departments and agencies in their responses to activities that undermine the security of Canada, and for working with industry to implement appropriate transportation security measures.

The Federal Terrorism Response Plan enumerates TC's core responsibilities as they pertain to counter-terrorism:

- Manage the security clearance program for access to restricted areas in airports and ports;
- Identify and respond to threats to aviation, marine and surface transportation;
- Develop and enforce security legislation, regulations and policy for the national transportation system;



- Monitor air, marine and rail/surface issues affecting the safety and security of the Canadian transportation system;
- Provide security support (including intelligence) to Transport Canada stakeholders;
- Ensure the implementation of transportation security measures as appropriate for aviation, marine and rail/surface; and,
- Regulate the transportation and handling of dangerous goods.

The Minister of Transport's areas of responsibility with respect to security are defined across a suite of lawful authorities that are typically specific to each mode of transportation – aviation, marine, rail/surface – or the transportation of dangerous goods.

## Financial Transactions and Reports Analysis Centre of Canada

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) facilitates the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while ensuring the protection of personal information under its control.

FINTRAC fulfills this mandate by:

- Receiving financial transaction reports and voluntary information in accordance with the legislation and regulations;
- Ensuring the compliance of reporting entities with the legislation and regulations;
- Producing financial intelligence relevant to investigations and prosecutions of money laundering, terrorist activity financing and threats to the security of Canada;
- Researching and analyzing data from a variety of information sources that shed light on trends and patterns in money laundering and the financing of terrorist activities;
- Maintaining a registry of money services businesses in Canada; and,
- Enhancing public awareness and understanding of money laundering and terrorist activity financing.

In fulfilling its mandate under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), FINTRAC must make a disclosure of designated information to the appropriate police service when it has reasonable grounds to suspect that the information to be disclosed would be relevant to the investigation or prosecution of a money laundering or terrorist activity financing offence. This same information relevant to a terrorist activity financing offence must be disclosed to the Canada Revenue Agency (CRA), Canada Border Services Agency (CBSA), Communications Security Establishment (CSE), and an agency or body that administers the securities legislation of a province, when a secondary threshold relevant to each agency is also met [PCMLTFA, s. 55 (3)].



FINTRAC must make a disclosure of designated information to the Canadian Security Intelligence Service (CSIS) when it has reasonable grounds to suspect that the information to be disclosed would be relevant to threats to the security of Canada. When a separate threshold with respect to each agency is met, FINTRAC must disclose the same information to the appropriate police service, the Canada Border Services Agency (CBSA) or the Department of National Defence (DND) [PCMLTFA, s. 55.1 (1)].

FINTRAC works with foreign financial intelligence units to protect Canadians and the integrity of Canada's financial system. Through bilateral agreements, the Centre is able to disclose financial intelligence to financial intelligence units worldwide when it has reasonable grounds to suspect that its intelligence would be relevant to the investigation or prosecution of a money laundering or a terrorist activity financing offence, or an offence that is substantially similar to either offence [PCMLTFA, s. 56 (1), 56 (2), 56 (3) & 56.1].

FINTRAC may conduct research into trends and developments in the area of the financing of terrorist activities and of improved ways of detecting, preventing and deterring the financing of terrorist activities. Furthermore, FINTRAC may inform the public and authorities engaged in the investigation and prosecution of money laundering and terrorist activity financing offences, and others, with respect to the nature and extent of the financing of terrorist activities inside and outside Canada, and measures to detect, prevent and deter the financing of terrorist activities inside and outside Canada, as well as the effectiveness of those measures [PCMLTFA, s. 58 (1)].

In its strategic intelligence products, FINTRAC cannot disclose any information that would, directly or indirectly, identify an individual who provided a report or information to FINTRAC, or a person or entity about whom a report or information was provided [PCMLTFA, s. 58 (2)]

## Public Health Agency of Canada

PHAC's national security activities include: surveillance for diseases and events resulting from the use of chemical, biological, radiological, nuclear and explosives (CBRNE) agents; coordination of public health response through activation of the Health Portfolio Emergency Operations Centre; maintenance of the National Emergency Stockpile System, which contains medical countermeasures against CBRNE agents and disaster medical supplies for use in mass casualty events; maintenance of Health Emergency Response Teams to provide surge capacity to provinces and territories; development of training and exercises to help prepare first responders and the health sector to respond to terrorism events involving the use of CBRNE

agents; regulating the importation and use of dangerous pathogens to prevent their importation and use by terrorists; and international collaboration with public health partners on issues related to health security.

## Royal Canadian Mounted Police

The Royal Canadian Mounted Police's (RCMP) mandate includes:

- preventing and investigating crime;
- maintaining peace and order;
- enforcing laws;
- contributing to national security;
- ensuring the safety of state officials, visiting dignitaries and foreign missions;
- providing vital operational support services to other police and law enforcement agencies within Canada and abroad [Royal Canadian Mounted Police Act, s. 18].

The RCMP's national security-related mandates and responsibilities range from national security criminal investigations, including those related to terrorism and foreign actor interference, to critical incident management and protective policing. They are the primary responsibility of the Federal Policing business line, with support from Specialized Policing Services.

### Responsibilities:

**Federal Policing:** Under the authority of the RCMP Act and the RCMP Regulations, Federal Policing enforces federal laws and protects Canada's institutions, national security and Canadian and foreign dignitaries by:

- enforcing federal statutes;
- collecting criminal intelligence;
- conducting criminal investigations;
- securing Canada's border;
- ensuring the safety of major events, state officials, Canadian and foreign dignitaries and foreign missions.

The Federal Policing Program preserves public safety and the integrity of Canada's political and economic systems by investigating serious and organized crime, financial crime, cybercrime, and other criminal activity that may pose a threat to the security of Canada such as terrorism, foreign actor interference, espionage and proliferation.

**Specialized Policing Services:** Specialized Policing Services includes Technical Services and Operational Support (Technical Operations), which provides direct specialized investigative and operational services to frontline police officers. The specialized investigative units also provide advice to RCMP senior management and other government agencies in the areas of corporate, information and government security. Technical Operations encompasses a variety of special investigative services and provides state-of-the-art technological tools for the RCMP and other law enforcement agencies to assist in investigations. This includes the lawfully authorized interception of communications, covert entry and surveillance, seizure and analysis of digital devices.

**Terrorism-Related Investigations:** The Criminal Code defines most criminal offences, including terrorism, with the *Anti-Terrorism Act*, 2001. The Code includes definitions and offences for terrorism:

- Interpretation [s. 83.01],
- Financing of Terrorism [s. 83.02],
- List of Entities [s. 83.05],
- Participating, Facilitating, Instructing and Harboring [s. 83.18],
- Recognizance with Conditions [s. 83.3].

Many tools used by foreign actors are otherwise illegal, and can be investigated by law enforcement. For example, regardless of who is doing it and why, mischief concerning computer data (i.e. hacking), bribery and harassment are within the mandate of Canadian police to investigate if the offence occurred in Canada.

**Protecting Sensitive Information:** The *Security of Information Act* (SOIA) permanently (for life) binds current and/or former employees and non-employees who are or have been privy to Special Operational Information (operationally sensitive government information) that the Government of Canada is taking measures to safeguard. The SOIA provides a legal framework for the RCMP to investigate cases of state-sponsored espionage related to any Government of Canada department, agency or body, the mishandling of special operational information, investigations related to persons bound to secrecy, and offences for communication of safeguarded information. The SOIA also addresses the use of trade secrets for the benefit of foreign economic entities, as well as conspiracy, and foreign-influenced or terrorist influenced threats of violence.

**Law Enforcement vis-à-vis Threats to the Security of Canada:** The RCMP is the primary law enforcement body in relation to alleged offences arising out of conduct constituting a threat to the security of Canada within the meaning of the Canadian Security Intelligence

Service Act, including offences related to terrorism, foreign actor interference and espionage, as well as for offences against internationally protected persons, such as foreign ambassadors accredited to Canada [*Security Offences Act*, s. 6 (1)].

**Review of Foreign Investments:** Pursuant to the *Investment Canada Act* (ICA), the RCMP is a Prescribed Investigative Body under s. 7 of the National Security Review of Investments Regulations, and is mandated to participate in the review of foreign investments to determine if there is any possible injury to Canada. The Ministers of Innovation, Science and Economic Development Canada may communicate or disclose “privileged information” to the RCMP if the communication or disclosure is for the purposes of the administration or enforcement of Part IV.1 of the ICA and that body’s lawful investigations. The information may also be communicated or disclosed by that body for the purposes of those investigations.

# Appendix E

## Heads of the Designated Recipient Institutions and/or Person(s) Designated by them

Every Government of Canada institution has its own standards and procedures for receiving information. For your reference, below is a list of the heads of the designated recipient institutions under the SCIDA and the persons designated by them to receive information. To disclose information under the SCIDA, it is strongly recommended that you contact the designated recipient institutions in advance to confirm you have the most appropriate point of contact.

### CANADA BORDER SERVICES AGENCY

**Head:**

- President of the Canada Border Services Agency

**Person Designated by the Head:**

- Intelligence Tactical Operations Centre (ITOC)  
[ITOC.COTR@cbsa-asfc.gc.ca](mailto:ITOC.COTR@cbsa-asfc.gc.ca)

For federal institutions wishing to disclose information to the Canada Border Services Agency (CBSA), and where those institutions do not already have an established national security point of contact within the CBSA, these institutions may contact the ITOC.

This mailbox can transmit communication up to Protected B, including Entrust encryption. For anything beyond Protected B, please contact the ITOC for further instructions.

## CANADA REVENUE AGENCY

### Head:

- Commissioner of Revenue

### Person Designated by the Head:

- Director, Review and Analysis Division, Charities Directorate  
Telephone: 613-954-2056
- Liaison, Review and Analysis Division, Charities Directorate  
Telephone: 613-952-9215  
Email: [LPCHRADLIAG@cra-arc.gc.ca](mailto:LPCHRADLIAG@cra-arc.gc.ca)

## CANADIAN FOOD INSPECTION AGENCY

### Head:

- President of the Canadian Food Inspection Agency  
Telephone: 613-773-6000

### Person Designated by the Head:

- N/A

## CANADIAN NUCLEAR SAFETY COMMISSION

### Head:

- President of the Canadian Nuclear Safety Commission

### Person Designated by the Head:

- Team Leader, Nuclear Security Support Operations, Nuclear Security Division, Directorate of Security and Safeguards  
Telephone: 613-943-9929  
Email: [cnsn.nuclearsecurity-securitenucleaire.ccsn@canada.ca](mailto:cnsn.nuclearsecurity-securitenucleaire.ccsn@canada.ca)

## CANADIAN SECURITY INTELLIGENCE SERVICE

### Head:

- Director of the Canadian Security Intelligence Service

### Person Designated by the Head:

- For proactive disclosures, please contact:  
CSIS Global Operations Centre  
Telephone: 613-993-9620  
Email: [ttc@smtp.gc.ca](mailto:ttc@smtp.gc.ca)

## COMMUNICATIONS SECURITY ESTABLISHMENT

### Head:

- Chief of the Communications Security Establishment

### Person Designated by the Head:

- Director, Disclosure and Information Sharing
- For proactive disclosures, please contact:  
Email: [SCIDA.LCISC@cse-cst.gc.ca](mailto:SCIDA.LCISC@cse-cst.gc.ca)

The Communications Security Establishment (CSE) may not direct its foreign intelligence activities toward Canadians or persons in Canada. Please disclose foreign lead information only. Organizations with an established national security contact at CSE should continue to use those pre-established channels.

This inbox can transmit communications up to Protected B, including Entrust Encryption. Please notify us if you wish to disclose information classified higher than Protected B.

**IMMIGRATION,  
REFUGEES, AND  
CITIZENSHIP  
CANADA**

**Head:**

- Minister of Immigration, Refugees and Citizenship

**Person Designated by the Head:**

- Assistant Director, Investigations and Exceptional Cases Division, Case Management Branch  
Telephone: 613-437-6367  
Email: [IRCC.CMBSecurity-SecuriteDGRC.IRCC@cic.gc.ca](mailto:IRCC.CMBSecurity-SecuriteDGRC.IRCC@cic.gc.ca)

**FINANCE CANADA**

**Head:**

- Minister of Finance

**Person Designated by the Head:**

- Assistant Deputy Minister, Financial Sector Policy Branch  
Telephone: 613-369-3620

**GLOBAL AFFAIRS  
CANADA**

**Head:**

- Minister of Foreign Affairs

**Person Designated by the Head:**

- UNCLASSIFIED information:  
[SCISA.DCC@international.gc.ca](mailto:SCISA.DCC@international.gc.ca)
- SECRET information can be forwarded by C6 to:  
[DCCSCISA.LCISC@c.international.gc.ca](mailto:DCCSCISA.LCISC@c.international.gc.ca)



## HEALTH CANADA

### Head:

- Minister of Health

### Person Designated by the Head:

- Assistant Deputy Minister, Healthy Environments and Consumer Safety Branch  
Telephone: 613-946-6701  
Email: [HECSB\\_Briefing@hc-sc.gc.ca](mailto:HECSB_Briefing@hc-sc.gc.ca)
- Executive Assistant to ADM: 613-946-6700
- Director of ADMO: 613-946-6705

## DEPARTMENT OF NATIONAL DEFENCE / CANADIAN ARMED FORCES

### Head:

- Minister of National Defence (DND)
- Chief of the Defence Staff (CAF)

### Person Designated by the Head:

- Release and Disclosure Coordination Office (DND/CAF)  
Telephone: 613-945-6307  
Unclassified Email: [RDCO.CFINTCOM@forces.gc.ca](mailto:RDCO.CFINTCOM@forces.gc.ca)  
Classified Email: [CFINTCOM\\_RDCO@spartan.mil.ic.ca](mailto:CFINTCOM_RDCO@spartan.mil.ic.ca)
- Canadian Forces Integrated Command Centre (24/7)  
Telephone: 613-998-4136  
Unclassified Email: [cficc@forces.gc.ca](mailto:cficc@forces.gc.ca)  
Classified Email: [cficc-ccifc@forces.cmil.ca](mailto:cficc-ccifc@forces.cmil.ca)

## DEPARTMENT OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS

### Head:

- Minister of Public Safety and Emergency Preparedness

### Person Designated by the Head:

- Director General, National Security Policy Directorate  
Telephone: 613-991-9170
  - For the Passenger Protect Program, passport decisions related to national security, and for national security immigration.
- Director General, National Security Operations Directorate  
Telephone: 613-993-4595
  - For information relating to the *Investment Canada Act*, terrorist entities listings, and state supporters of terrorism listings.
- Director General, Cyber Security Directorate  
Telephone: 613-990-2661
  - For cyber security matters.
- Director General, Critical Infrastructure and Strategic Coordination Directorate  
Telephone: 613-991-3583
  - For critical infrastructure matters.
- Government Operations Centre  
Telephone: 613-993-7233
  - For urgent 24/7 response to events or issues that affect, or may affect, Canada's national interests, including national security and cyber events.

## TRANSPORT CANADA

**Head:**

- Minister of Transport

**Person Designated by the Head:**

- Director, Security Intelligence Assessment Branch  
Telephone: 613-990-1812  
Email: [SCIDA-LCISC@tc.gc.ca](mailto:SCIDA-LCISC@tc.gc.ca)

## FINANCIAL TRANSACTIONS AND REPORTS ANALYSIS CENTRE OF CANADA

**Head:**

- Director and Chief Executive Officer of the Financial Transactions and Reports Analysis Centre of Canada

**Person Designated by the Head:**

- Manager, Operational Integration and Support, Operations  
Email: [partner-partenaire@fintrac-canafe.gc.ca](mailto:partner-partenaire@fintrac-canafe.gc.ca)

## PUBLIC HEALTH AGENCY OF CANADA

**Head:**

- Chief Public Health Officer and President of the Public Health Agency of Canada

**Person Designated by the Head:**

- Branch Head, Health Security Infrastructure Branch  
Telephone: 613-957-0316
- Executive Director, Centre for Emergency Preparedness and Response, Health Security Infrastructure Branch  
Telephone: 613-941-6084

## ROYAL CANADIAN MOUNTED POLICE

### Head:

- Commissioner of the Royal Canadian Mounted Police

### Person Designated by the Head:

- Federal Policing Intake Unit  
Telephone: 613-843-3400  
Email: [Federal\\_Policing\\_Intake\\_Unit\\_ML@rcmp-grc.gc.ca](mailto:Federal_Policing_Intake_Unit_ML@rcmp-grc.gc.ca)

The Commissioner of the Royal Canadian Mounted Police (RCMP) is authorized to receive disclosures under the *Security of Canada Information Disclosure Act (SCIDA)*. This authority has been delegated to 13 designated officials, including the Director General of Federal Policing National Security, the Director of Federal Policing National Security, and the Officer in Charge of the National Security Joint Operations Centre. Disclosures to the RCMP must be addressed to the Commissioner or a designated official, and routed through the Federal Policing Intake Unit point of contact provided above.

# **Appendix F**

## *Security of Canada Information Disclosure Act*



CANADA

CONSOLIDATION

CODIFICATION

## Security of Canada Information Disclosure Act

## Loi sur la communication d'information ayant trait à la sécurité du Canada

S.C. 2015, c. 20, s. 2

L.C. 2015, ch. 20, art. 2

### NOTE

[Enacted by section 2 of chapter 20 of the Statutes of Canada, 2015, in force August 1, 2015, *see* SI/2015-64.]

### NOTE

[Édictée par l'article 2 du chapitre 20 des Lois du Canada (2015), en vigueur le 1<sup>er</sup> août 2015, *voir* TR/2015-64.]

Current to November 19, 2019

Last amended on August 1, 2019

À jour au 19 novembre 2019

Dernière modification le 1 août 2019

---

## OFFICIAL STATUS OF CONSOLIDATIONS

Subsections 31(1) and (2) of the *Legislation Revision and Consolidation Act*, in force on June 1, 2009, provide as follows:

### Published consolidation is evidence

**31 (1)** Every copy of a consolidated statute or consolidated regulation published by the Minister under this Act in either print or electronic form is evidence of that statute or regulation and of its contents and every copy purporting to be published by the Minister is deemed to be so published, unless the contrary is shown.

### Inconsistencies in Acts

**(2)** In the event of an inconsistency between a consolidated statute published by the Minister under this Act and the original statute or a subsequent amendment as certified by the Clerk of the Parliaments under the *Publication of Statutes Act*, the original statute or amendment prevails to the extent of the inconsistency.

## LAYOUT

The notes that appeared in the left or right margins are now in boldface text directly above the provisions to which they relate. They form no part of the enactment, but are inserted for convenience of reference only.

## NOTE

This consolidation is current to November 19, 2019. The last amendments came into force on August 1, 2019. Any amendments that were not in force as of November 19, 2019 are set out at the end of this document under the heading “Amendments Not in Force”.

## CARACTÈRE OFFICIEL DES CODIFICATIONS

Les paragraphes 31(1) et (2) de la *Loi sur la révision et la codification des textes législatifs*, en vigueur le 1<sup>er</sup> juin 2009, prévoient ce qui suit :

### Codifications comme élément de preuve

**31 (1)** Tout exemplaire d'une loi codifiée ou d'un règlement codifié, publié par le ministre en vertu de la présente loi sur support papier ou sur support électronique, fait foi de cette loi ou de ce règlement et de son contenu. Tout exemplaire donné comme publié par le ministre est réputé avoir été ainsi publié, sauf preuve contraire.

### Incompatibilité – lois

**(2)** Les dispositions de la loi d'origine avec ses modifications subséquentes par le greffier des Parlements en vertu de la *Loi sur la publication des lois* l'emportent sur les dispositions incompatibles de la loi codifiée publiée par le ministre en vertu de la présente loi.

## MISE EN PAGE

Les notes apparaissant auparavant dans les marges de droite ou de gauche se retrouvent maintenant en caractères gras juste au-dessus de la disposition à laquelle elles se rattachent. Elles ne font pas partie du texte, n'y figurant qu'à titre de repère ou d'information.

## NOTE

Cette codification est à jour au 19 novembre 2019. Les dernières modifications sont entrées en vigueur le 1 août 2019. Toutes modifications qui n'étaient pas en vigueur au 19 novembre 2019 sont énoncées à la fin de ce document sous le titre « Modifications non en vigueur ».

## TABLE OF PROVISIONS

**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**

	<b>Short Title</b>
1	Short title
	<b>Interpretation</b>
2	Definitions
	<b>Purpose and Principles</b>
3	Purpose
4	Guiding principles
	<b>Disclosure of Information</b>
5	Disclosure of information to institution listed in Schedule 3
5.1	Requirement to destroy or return
6	Clarification
7	No presumption
7.1	Clarification
8	Non-derogation
	<b>Record Keeping</b>
9	Obligation — disclosing institution
	<b>Powers of Governor in Council</b>
10	Regulations
	<b>SCHEDULE 1</b>
	Excluded Institutions
	<b>SCHEDULE 2</b>
	Additional Institutions
	<b>SCHEDULE 3</b>

## TABLE ANALYTIQUE

**Loi visant à encourager et à faciliter la communication d'information entre les institutions fédérales afin de protéger le Canada contre des activités qui portent atteinte à la sécurité du Canada**

	<b>Titre abrégé</b>
1	Titre abrégé
	<b>Définitions</b>
2	Définitions
	<b>Objet et principes</b>
3	Objet
4	Principes directeurs
	<b>Communication d'information</b>
5	Communication d'information à une institution figurant à l'annexe 3
5.1	Destruction ou remise
6	Précision
7	Aucune présomption
7.1	Précision
8	Aucune dérogation
	<b>Conservation de documents</b>
9	Obligation : institution fédérale qui communique
	<b>Pouvoirs du gouverneur en conseil</b>
10	Règlements
	<b>ANNEXE 1</b>
	Institutions exclues
	<b>ANNEXE 2</b>
	Institutions supplémentaires
	<b>ANNEXE 3</b>





S.C. 2015, c. 20, s. 2

**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**

[Assented to 18th June 2015]

**Preamble**

Whereas the people of Canada are entitled to live free from threats to their lives and their security;

Whereas activities that undermine the security of Canada are often carried out in a clandestine, deceptive or hostile manner, are increasingly global, complex and sophisticated, and often emerge and evolve rapidly;

Whereas there is no more fundamental role for a government than protecting its country and its people;

Whereas Canada is not to be used as a conduit for the carrying out of activities that threaten the security of another state;

Whereas protecting Canada and its people against activities that undermine the security of Canada often transcends the mandate and capability of any one Government of Canada institution;

Whereas Parliament recognizes that information needs to be disclosed — and disparate information needs to be collated — in order to enable the Government to protect Canada and its people against activities that undermine the security of Canada;

Whereas Government of Canada institutions are accountable for the effective and responsible disclosure of information in a manner that respects the *Canadian Charter of Rights and Freedoms*, the *Privacy Act* and other laws regarding the protection of privacy;

L.C. 2015, ch. 20, art. 2

**Loi visant à encourager et à faciliter la communication d'information entre les institutions fédérales afin de protéger le Canada contre des activités qui portent atteinte à la sécurité du Canada**

[Sanctionnée le 18 juin 2015]

**Préambule**

Attendu :

que la population du Canada est en droit de vivre à l'abri des menaces à la vie ou à la sécurité;

que les activités portant atteinte à la sécurité du Canada sont souvent menées de manière clandestine, trompeuse ou hostile, sont de plus en plus globales, complexes et sophistiquées, et voient le jour et évoluent souvent rapidement;

qu'il n'est point de rôle plus fondamental pour un gouvernement que la protection de son pays et de sa population;

que le Canada ne doit pas servir d'intermédiaire à quiconque mène des activités qui menacent la sécurité d'un État étranger;

que la protection du Canada et de sa population contre des activités portant atteinte à la sécurité du Canada excède souvent le mandat ou les capacités d'une seule institution fédérale;

que le Parlement reconnaît la nécessité de communiquer de l'information — et de regrouper des éléments d'information disparates — pour permettre au gouvernement de protéger le Canada et sa population contre ces activités;

que les institutions fédérales sont garantes d'une communication d'information responsable et efficace effectuée d'une manière qui respecte la *Charte canadienne des droits et libertés*, la *Loi sur la*

And whereas an explicit authority will facilitate the effective and responsible disclosure of information to protect the security of Canada;

Now, therefore, Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows:

## Short Title

### Short title

**1** This Act may be cited as the *Security of Canada Information Disclosure Act*.

2015, c. 20, s. 2 "1"; 2019, c. 13, s. 114(E).

## Interpretation

### Definitions

**2 (1)** The following definitions apply in this Act.

#### **activity that undermines the security of Canada**

means any activity that undermines the sovereignty, security or territorial integrity of Canada or threatens the lives or the security of people in Canada or of any individual who has a connection to Canada and who is outside Canada. For greater certainty, it includes

- (a)** interference with the capability of the Government of Canada in relation to intelligence, defence, border operations or public safety;
- (b)** changing or unduly influencing a government in Canada by force or unlawful means;
- (c)** espionage, sabotage or covert foreign-influenced activities;
- (d)** terrorism;
- (e)** proliferation of nuclear, chemical, radiological or biological weapons;
- (f)** significant or widespread interference with critical infrastructure;
- (g)** significant or widespread interference with the *global information infrastructure*, as defined in section 2 of the *Communications Security Establishment Act*; and

*protection des renseignements personnels* et les autres lois relatives à la protection de la vie privée;

qu'un pouvoir explicite facilitera la communication d'information responsable et efficace, de façon à protéger la sécurité du Canada,

Sa Majesté, sur l'avis et avec le consentement du Sénat et de la Chambre des communes du Canada, édicte :

## Titre abrégé

### Titre abrégé

**1** *Loi sur la communication d'information ayant trait à la sécurité du Canada*.

2015, ch. 20, art. 2 « 1 »; 2019, ch. 13, art. 114(A).

## Définitions

### Définitions

**2 (1)** Les définitions qui suivent s'appliquent à la présente loi.

#### **activité portant atteinte à la sécurité du Canada**

Activité qui porte atteinte à la souveraineté, à la sécurité ou à l'intégrité territoriale du Canada ou qui menace la vie ou la sécurité de la population au Canada ou de toute personne physique qui a un lien avec le Canada et qui se trouve à l'étranger. Il est entendu que les activités ci-après sont comprises dans la présente définition :

- a)** entraver la capacité du gouvernement fédéral — ou de son administration — en matière de renseignement, de défense, d'activités à la frontière ou de sécurité publique;
- b)** entraîner un changement de gouvernement au Canada ou influencer indûment sur un tel gouvernement par l'emploi de la force ou de moyens illégaux;
- c)** espionner, saboter ou se livrer à une activité secrète influencée par l'étranger;
- d)** se livrer au terrorisme;
- e)** se livrer à une activité qui a pour effet la prolifération d'armes nucléaires, chimiques, radiologiques ou biologiques;
- f)** entraver de manière considérable ou à grande échelle le fonctionnement d'infrastructures essentielles;

**(h)** conduct that takes place in Canada and that undermines the security of another state. (*activité portant atteinte à la sécurité du Canada*)

**(i)** [Repealed, 2019, c. 13, s. 115]

**Government of Canada institution** means

**(a)** a government institution — as defined in section 3 of the *Privacy Act* — other than one that is listed in Schedule 1; or

**(b)** an institution that is listed in Schedule 2. (*institution fédérale*)

**people of Canada** [Repealed, 2019, c. 13, s. 115]

### Exception

**(2)** For the purposes of this Act, advocacy, protest, dissent or artistic expression is not an activity that undermines the security of Canada unless carried on in conjunction with an activity that undermines the security of Canada.

2015, c. 20, s. 2 "2"; 2019, c. 13, s. 89; 2019, c. 13, s. 115.

## Purpose and Principles

### Purpose

**3** The purpose of this Act is 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.

2015, c. 20, s. 2 "3"; 2019, c. 13, s. 116(E).

### Guiding principles

**4** The disclosure of information under this Act is to be guided by the following principles:

**(a)** effective and responsible disclosure of information protects Canada and Canadians;

**(b)** respect for caveats on and originator control over disclosed information is consistent with effective and responsible disclosure of information;

**(c)** entry into an information-sharing arrangement is appropriate when a Government of Canada institution

**g)** entraver de manière considérable ou à grande échelle le fonctionnement de l'*infrastructure mondiale de l'information*, au sens de l'article 273.61 de la *Loi sur la défense nationale*;

**h)** adopter au Canada une conduite qui porte atteinte à la sécurité d'un autre État. (*activity that undermines the security of Canada*)

**i)** [Abrogé, 2019, ch. 13, art. 115]

**institution fédérale** S'entend :

**a)** de l'institution fédérale, au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*, autre qu'une institution qui figure à l'annexe 1;

**b)** d'une institution qui figure à l'annexe 2. (*Government of Canada institution*)

**population du Canada** [Abrogée, 2019, ch. 13, art. 115]

### Exception

**(2)** Pour l'application de la présente loi, sauf si elles ont un lien avec une activité portant atteinte à la sécurité du Canada, les activités de défense d'une cause, de protestation, de manifestation d'un désaccord ou d'expression artistique ne sont pas des activités portant atteinte à la sécurité du Canada.

2015, ch. 20, art. 2 « 2 »; 2019, ch. 13, art. 89; 2019, ch. 13, art. 115.

## Objet et principes

### Objet

**3** La présente loi a pour objet d'encourager les institutions fédérales à communiquer entre elles de l'information et de faciliter une telle communication, afin de protéger le Canada contre des activités portant atteinte à la sécurité du Canada.

2015, ch. 20, art. 2 « 3 »; 2019, ch. 13, art. 116(A).

### Principes directeurs

**4** Les principes ci-après doivent guider la communication d'information au titre de la présente loi :

**a)** la communication d'information responsable et efficace protège le Canada et les Canadiens;

**b)** le respect des mises en garde et du droit de regard de la source relativement à l'information ainsi communiquée est compatible avec une communication d'information responsable et efficace;

**c)** la conclusion d'une entente de communication d'information convient lorsqu'une institution fédérale

regularly discloses information to the same Government of Canada institution;

**(d)** the provision of feedback as to how disclosed information is used and as to whether it is useful in protecting against activities that undermine the security of Canada facilitates effective and responsible information disclosure; and

**(e)** only those within an institution who exercise its jurisdiction or carry out its responsibilities in respect of activities that undermine the security of Canada ought to receive information that is disclosed under this Act.

2015, c. 20, s. 2 "4"; 2019, c. 13, s. 117.

## Disclosure of Information

### Disclosure of information to institution listed in Schedule 3

**5 (1)** Subject to any provision of any other Act of Parliament, or of any regulation made under such an Act, that prohibits or restricts the disclosure of information, a Government of Canada institution may, on its own initiative or on request, disclose information to the head of a recipient Government of Canada institution whose title is listed in Schedule 3, or to a person designated by the head of that recipient institution, if the disclosing institution is 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, in respect of activities that undermine the security of Canada; and

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

### Statement regarding accuracy and reliability

**(2)** An 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.

2015, c. 20, s. 2 "5"; 2019, c. 13, s. 118.

### Requirement to destroy or return

**5.1 (1)** A Government of Canada 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

communiqué régulièrement de l'information à la même institution fédérale;

**d)** la fourniture de rétroaction sur la façon dont l'information qui est communiquée est utilisée et sur son utilité en matière de protection contre des activités portant atteinte à la sécurité du Canada facilite une communication d'information responsable et efficace;

**e)** seuls ceux qui, au sein d'une institution, exercent la compétence ou les attributions de celle-ci à l'égard d'activités portant atteinte à la sécurité du Canada devraient recevoir l'information communiquée en vertu de la présente loi.

2015, ch. 20, art. 2 « 4 »; 2019, ch. 13, art. 117.

## Communication d'information

### Communication d'information à une institution figurant à l'annexe 3

**5 (1)** Sous réserve des dispositions de toute autre loi fédérale ou de tout règlement pris en vertu de l'une de celles-ci interdisant ou restreignant la communication d'information, une institution fédérale peut, de sa propre initiative ou sur demande, communiquer de l'information au responsable d'une institution fédérale destinataire dont le titre figure à l'annexe 3, ou à la personne que le responsable de l'institution fédérale destinataire désigne, si elle est convaincue :

**a)** que la communication aidera à l'exercice de la compétence ou des attributions de l'institution fédérale destinataire prévues par une loi fédérale ou une autre autorité légitime à l'égard d'activités portant atteinte à la sécurité du Canada;

**b)** que l'incidence de la communication sur le droit à la vie privée d'une personne sera limitée à ce qui est raisonnablement nécessaire dans les circonstances.

### Déclaration concernant l'exactitude et la fiabilité

**(2)** L'institution qui communique de l'information en vertu du paragraphe (1) doit également fournir, au moment de la communication, des renseignements sur l'exactitude de l'information et la fiabilité quant à la façon dont celle-ci a été obtenue.

2015, ch. 20, art. 2 « 5 »; 2019, ch. 13, art. 118.

### Destruction ou remise

**5.1 (1)** L'institution fédérale détruit ou remet à l'expéditeur, dès que possible après leur réception, les *renseignements personnels*, au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*, qui lui sont communiqués au titre de l'article 5 et qui ne sont

responsibilities, under an Act of Parliament or another lawful authority, in respect of activities that undermine the security of Canada.

### Exception

**(2)** Subsection (1) does not apply if the retention of the information is required by law.

### *Canadian Security Intelligence Service Act*

**(3)** Subsection (1) 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*.

2019, c. 13, s. 118.

### Clarification

**6** Nothing in section 5 or 5.1 is to be construed as authorizing the collection or use of any information that is disclosed under section 5.

2015, c. 20, s. 2 "6"; 2019, c. 13, s. 118.

### No presumption

**7** The act of disclosing information under this Act does not create a presumption

**(a)** that the disclosing institution is conducting a joint investigation or decision-making process with the recipient institution and therefore has the same obligations, if any, as the recipient institution to disclose or produce information for the purposes of a proceeding; or

**(b)** that there has been a waiver of any privilege, or of any requirement to obtain consent, for the purposes of any other disclosure of that information either in a proceeding or to an institution that is not a Government of Canada institution.

### Clarification

**7.1** For greater certainty, for the purpose of paragraph 8(2)(b) of the *Privacy Act*, the authority in this Act to disclose information includes the authority to disclose *personal information*, as defined in section 3 of the *Privacy Act*.

2019, c. 13, s. 118.1.

pas nécessaires à l'exercice de sa compétence ou de ses attributions prévues par une loi fédérale ou une autre autorité légitime à l'égard d'activités portant atteinte à la sécurité du Canada.

### Exception

**(2)** Le paragraphe (1) ne s'applique pas si la conservation de ces renseignements est légalement exigée.

### *Loi sur le Service canadien du renseignement de sécurité*

**(3)** Le paragraphe (1) ne s'applique pas au Service canadien du renseignement de sécurité à l'égard de ceux de ces renseignements qui se rapportent à l'exercice de ses fonctions aux termes de l'article 12 de la *Loi sur le Service canadien du renseignement de sécurité*.

2019, ch. 13, art. 118.

### Précision

**6** Les articles 5 et 5.1 n'ont pas pour effet d'autoriser la collecte ou l'utilisation de l'information communiquée au titre de l'article 5.

2015, ch. 20, art. 2 « 6 »; 2019, ch. 13, art. 118.

### Aucune présomption

**7** Le fait de communiquer de l'information au titre de la présente loi ne crée pas de présomption selon laquelle :

**a)** l'institution la communiquant participe à une enquête ou à un processus décisionnel menés avec l'institution destinataire et a ainsi les mêmes obligations, le cas échéant, que cette dernière institution en matière de communication ou de production d'information dans le cadre d'une instance;

**b)** il y a eu renonciation à tout privilège ou à toute exigence d'obtenir un consentement aux fins de toute autre communication de cette information, que celle-ci soit communiquée dans le cadre d'une instance ou à une institution qui n'est pas une institution fédérale.

### Précision

**7.1** Il est entendu que, pour l'application de l'alinéa 8(2)b) de la *Loi sur la protection des renseignements personnels*, le pouvoir de communiquer de l'information au titre de la présente loi comprend celui de communiquer des *renseignements personnels*, au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*.

2019, ch. 13, art. 118.1.

### Non-derogation

**8** Nothing in this Act limits or affects any authority to disclose information under another Act of Parliament or a provincial Act, at common law or under the royal prerogative.

## Record Keeping

### Obligation — disclosing institution

**9 (1)** Every Government of Canada institution that discloses information under this Act must prepare and keep records that set out

- (a)** a description of the information;
- (b)** the name of the individual who authorized its disclosure;
- (c)** the name of the recipient Government of Canada institution;
- (d)** the date on which it was disclosed;
- (e)** a description of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under this Act; and
- (f)** any other information specified by the regulations.

### Obligation — recipient institution

**(2)** Every Government of Canada institution that receives information under this Act must prepare and keep records that set out

- (a)** a description of the information;
- (b)** the name of the institution that disclosed it;
- (c)** the name or position of the head of the recipient institution — or of the person designated by the head — who received the information;
- (d)** the date on which it was received by the recipient institution;
- (e)** whether the information has been destroyed or returned under subsection 5.1(1);
- (f)** if the information has been destroyed under subsection 5.1(1), the date on which it was destroyed;
- (g)** if the information was returned under subsection 5.1(1) to the institution that disclosed it, the date on which it was returned; and
- (h)** any other information specified by the regulations.

### Aucune dérogation

**8** La présente loi n'a pas pour effet de porter atteinte aux pouvoirs en matière de communication d'information qui découlent d'une autre loi fédérale, d'une loi provinciale, de la common law ou de la prérogative royale.

## Conservation de documents

### Obligation : institution fédérale qui communique

**9 (1)** L'institution fédérale qui communique de l'information en vertu de la présente loi prépare et conserve des documents qui contiennent les renseignements suivants :

- a)** une description de l'information communiquée;
- b)** le nom de la personne physique qui a autorisé la communication;
- c)** le nom de l'institution fédérale destinataire;
- d)** la date de la communication;
- e)** une description des renseignements sur lesquels l'institution fédérale s'est fondée pour conclure que la communication était autorisée par la présente loi;
- f)** tout autre renseignement précisé par règlement.

### Obligation : institution fédérale destinataire

**(2)** L'institution fédérale qui reçoit de l'information en vertu de la présente loi prépare et conserve des documents qui contiennent les renseignements suivants :

- a)** une description de l'information reçue;
- b)** le nom de l'institution fédérale qui l'a communiquée;
- c)** le nom ou le poste du responsable de l'institution fédérale destinataire, ou de la personne désignée par lui, qui a reçu l'information;
- d)** la date à laquelle l'information a été reçue par l'institution fédérale destinataire;
- e)** si l'information a été détruite ou remise au titre du paragraphe 5.1(1) ou non;
- f)** si l'information a été détruite au titre du paragraphe 5.1(1), la date de la destruction;
- g)** si l'information a été remise au titre du paragraphe 5.1(1) à l'institution fédérale qui l'a communiquée, la date de la remise;

### **Copy to National Security and Intelligence Review Agency**

**(3)** Within 30 days after the end of each calendar year, every Government of Canada institution that disclosed information under section 5 during the year and every Government of Canada institution that received such information must provide the National Security and Intelligence Review Agency with a copy of every record it prepared under subsection (1) or (2), as the case may be, with respect to the information.

2015, c. 20, s. 2 "9"; 2019, c. 13, s. 119.

## **Powers of Governor in Council**

### **Regulations**

**10 (1)** The Governor in Council may, on the recommendation of the Minister of Public Safety and Emergency Preparedness, make regulations for carrying out the purposes and provisions of this Act, including regulations

- (a)** respecting the manner of disclosure under section 5;
- (b)** specifying information for the purposes of paragraph 9(1)(f) or (2)(f); and
- (c)** respecting the manner in which records that are required by subsection 9(1) or (2) are to be prepared and kept and specifying the period during which they are to be kept.

### **Amendments to Schedules 1 and 2**

**(2)** The Governor in Council may make an order adding the name of an institution to Schedule 1 or 2 or deleting one from either of those Schedules.

### **Amendments to Schedule 3**

**(3)** The Governor in Council may make an order adding the name of a Government of Canada institution and the title of its head to Schedule 3, deleting the name of an institution and the title of its head from that Schedule or amending the name of an institution or the title of a head that is listed in that Schedule. An addition is authorized only if the institution has jurisdiction or responsibilities under an Act of Parliament or another lawful authority in respect of activities that undermine the security of Canada.

2015, c. 20, s. 2 "10"; 2019, c. 13, s. 120.

**h)** tout autre renseignement précisé par règlement.

### **Copie à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement**

**(3)** Dans les trente jours suivant la fin de chaque année civile, chaque institution fédérale qui a communiqué de l'information au titre de l'article 5 durant l'année et chaque institution fédérale qui l'a reçue fournit à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement une copie des documents préparés en application des paragraphes (1) ou (2) à l'égard de l'information.

2015, ch. 20, art. 2 « 9 »; 2019, ch. 13, art. 119.

## **Pouvoirs du gouverneur en conseil**

### **Règlements**

**10 (1)** Sur recommandation du ministre de la Sécurité publique et de la Protection civile, le gouverneur en conseil peut, par règlement, prendre toute mesure d'application de la présente loi, notamment des règlements :

- a)** concernant les modalités des communications faites en vertu de l'article 5;
- b)** précisant des renseignements pour l'application des alinéas 9(1)f) ou (2)f);
- c)** concernant les modalités de préparation et de conservation des documents exigés par les paragraphes 9(1) ou (2) et précisant leur période de conservation.

### **Modification des annexes 1 et 2**

**(2)** Le gouverneur en conseil peut, par décret, ajouter le nom d'une institution à l'annexe 1 ou 2 ou en supprimer un de l'une ou l'autre de ces annexes.

### **Modification de l'annexe 3**

**(3)** Le gouverneur en conseil peut, par décret, ajouter le nom d'une institution fédérale et le titre de son responsable à l'annexe 3, supprimer de cette annexe le nom d'une institution et le titre de son responsable ou modifier le nom d'une institution ou le titre d'un responsable qui figure à cette annexe. Il ne peut y avoir ajout que si l'institution est compétente ou a des attributions au titre d'une loi fédérale ou d'une autre autorité légitime à l'égard d'activités portant atteinte à la sécurité du Canada.

2015, ch. 20, art. 2 « 10 »; 2019, ch. 13, art. 120.

## **SCHEDULE 1**

(Section 2 and subsection 10(2))

# **Excluded Institutions**

## **ANNEXE 1**

(article 2 et paragraphe 10(2))

# **Institutions exclues**



## **SCHEDULE 2**

(Section 2 and subsection 10(2))

# **Additional Institutions**

2015, c. 20, s. 2 "Sch. 2"; 2019, c. 13, s. 73.

## **ANNEXE 2**

(article 2 et paragraphe 10(2))

# **Institutions supplémentaires**

2015, ch. 20, art. 2 « ann. 2 »; 2019, ch. 13, art. 73.

### SCHEDULE 3

(Subsections 5(1) and 10(3))

## Recipient Government of Canada Institutions and Their Heads

Column 1 Recipient Institution	Column 2 Head
Canada Border Services Agency <i>Agence des services frontaliers du Canada</i>	President of the Canada Border Services Agency
Canada Revenue Agency <i>Agence du revenu du Canada</i>	Commissioner of Revenue
Canadian Armed Forces <i>Forces armées canadiennes</i>	Chief of the Defence Staff
Canadian Food Inspection Agency <i>Agence canadienne d'inspection des aliments</i>	President of the Canadian Food Inspection Agency
Canadian Nuclear Safety Commission <i>Commission canadienne de sûreté nucléaire</i>	President of the Canadian Nuclear Safety Commission
Canadian Security Intelligence Service <i>Service canadien du renseignement de sécurité</i>	Director of the Canadian Security Intelligence Service
Communications Security Establishment <i>Centre de la sécurité des télécommunications</i>	Chief of the Communications Security Establishment
Department of Citizenship and Immigration <i>Ministère de la Citoyenneté et de l'Immigration</i>	Minister of Citizenship and Immigration
Department of Finance <i>Ministère des Finances</i>	Minister of Finance
Department of Foreign Affairs, Trade and Development <i>Ministère des Affaires étrangères, du Commerce et du Développement</i>	Minister of Foreign Affairs
Department of Health <i>Ministère de la Santé</i>	Minister of Health
Department of National Defence <i>Ministère de la Défense nationale</i>	Minister of National Defence
Department of Public Safety and Emergency Preparedness <i>Ministère de la Sécurité publique et de la Protection civile</i>	Minister of Public Safety and Emergency Preparedness
Department of Transport <i>Ministère des Transports</i>	Minister of Transport
Financial Transactions and Reports Analysis Centre of Canada <i>Centre d'analyse des opérations et déclarations financières du Canada</i>	Director of the Financial Transactions and Reports Analysis Centre of Canada

### ANNEXE 3

(paragraphe 5(1) et 10(3))

## Institutions fédérales destinataires et leurs responsables

Colonne 1 Institution destinataire	Colonne 2 Responsable
Agence canadienne d'inspection des aliments <i>Canadian Food Inspection Agency</i>	Le président de l'Agence canadienne d'inspection des aliments
Agence de la santé publique du Canada <i>Public Health Agency of Canada</i>	Le président de l'Agence de la santé publique du Canada
Agence des services frontaliers du Canada <i>Canada Border Services Agency</i>	Le président de l'Agence des services frontaliers du Canada
Agence du revenu du Canada <i>Canada Revenue Agency</i>	Le commissaire du revenu
Centre d'analyse des opérations et déclarations financières du Canada <i>Financial Transactions and Reports Analysis Centre of Canada</i>	Le directeur du Centre d'analyse des opérations et déclarations financières du Canada
Centre de la sécurité des télécommunications <i>Communications Security Establishment</i>	Le chef du Centre de la sécurité des télécommunications
Commission canadienne de sûreté nucléaire <i>Canadian Nuclear Safety Commission</i>	Le président de la Commission canadienne de sûreté nucléaire
Forces armées canadiennes <i>Canadian Armed Forces</i>	Le chef d'état-major de la défense
Gendarmerie royale du Canada <i>Royal Canadian Mounted Police</i>	Le commissaire de la Gendarmerie royale du Canada
Ministère de la Citoyenneté et de l'Immigration <i>Department of Citizenship and Immigration</i>	Le ministre de la Citoyenneté et de l'Immigration
Ministère de la Défense nationale <i>Department of National Defence</i>	Le ministre de la Défense nationale
Ministère de la Santé <i>Department of Health</i>	Le ministre de la Santé
Ministère de la Sécurité publique et de la Protection civile <i>Department of Public Safety and Emergency Preparedness</i>	Le ministre de la Sécurité publique et de la Protection civile
Ministère des Affaires étrangères, du Commerce et du Développement <i>Department of Foreign Affairs, Trade and Development</i>	Le ministre des Affaires étrangères

Column 1 Recipient Institution	Column 2 Head
Public Health Agency of Canada <i>Agence de la santé publique du Canada</i>	President of the Public Health Agency of Canada
Royal Canadian Mounted Police <i>Gendarmerie royale du Canada</i>	Commissioner of the Royal Canadian Mounted Police

2015, c. 20, ss. 2 "Sch. 3", 9.

Colonne 1 Institution destinataire	Colonne 2 Responsable
Ministère des Finances <i>Department of Finance</i>	Le ministre des Finances
Ministère des Transports <i>Department of Transport</i>	Le ministre des Transports
Service canadien du renseignement de sécurité <i>Canadian Security Intelligence Service</i>	Le directeur du Service canadien du renseignement de sécurité

2015, ch. 20, art. 2 « ann. 3 » et 9.

## RELATED PROVISIONS

— 2019, c. 13, par. 82(1)(e)

### References

**82 (1)** A reference to the former department in any of the following is deemed to be a reference to the new department:

(e) Schedule 3 to the *Security of Canada Information Disclosure Act*;

## DISPOSITIONS CONNEXES

— 2019, ch. 13, al. 82(1)e)

### Mentions

**82 (1)** La mention de l'ancien ministère dans les textes ci-après vaut mention du nouveau ministère :

e) l'annexe 3 de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*;