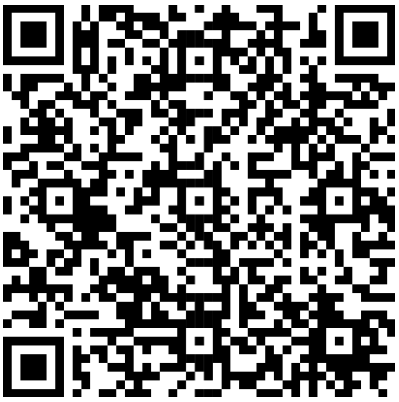
Public Safety Canada | Sécurité publique Canada

Canada



Security of Canada Information Disclosure Act (SCIDA): A Step-by-Step Guide to Responsible Information Sharing

2022



Read this publication online at:
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/scida-lcisc-2022/index-en.aspx

The step-by-step SCIDA Guide 2022 includes detailed advice on when and how to disclose national security information under the Security of Canada Information Disclosure Act (SCIDA), as well as an overview of the national security mandate of each recipient institution and a list of the heads of institutions, or persons designated to receive information within those institutions, where appropriate. The guide also updated templates for disclosing and receiving information under the SCIDA.

Aussi disponible en français sous le titre : Loi sur la communication d'information ayant trait à la sécurité du Canada (LCISC) : Un guide étape par étape sur la communication d'information responsable.

Public Safety Canada, Communications
269 Laurier Ave West
Ottawa ON K1A 0P8
Canada

communications@ps-sp.gc.ca

Catalogue Number: PS4-258/2023E-PDF

ISBN: 978-0-660-47936-1

Table of contents

Purpose

This guide is intended to help the reader navigate the *Security of Canada Information Disclosure Act* (SCIDA) and to facilitate the development of effective and responsible information disclosure practices between Government of Canada (GC) institutions.

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: scci-ccsi@ps-sp.gc.ca.

Public Safety Canada will continue to update this resource as needed and distribute new versions as they become available.

Background

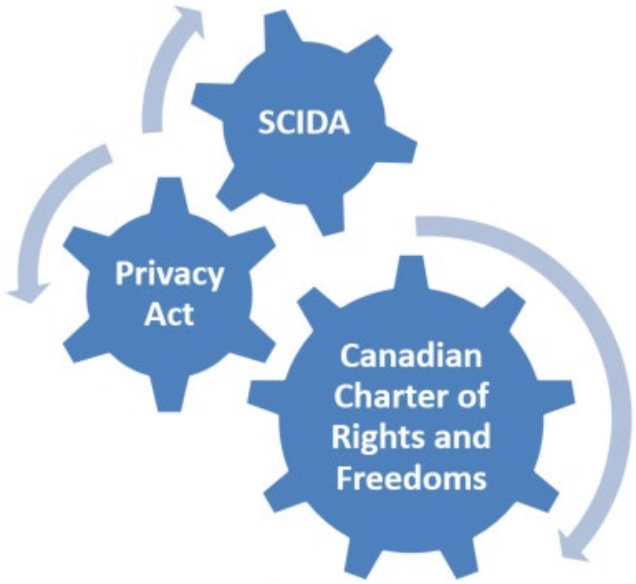
The *Security of Canada Information Disclosure Act* (*SCIDA*) was developed in the context of a comprehensive reform of Canada's national security framework in 2019. It is the second iteration of federal legislation aimed at encouraging and facilitating the disclosure of information for national security purposes between institutions of the Government of Canada. The first iteration was the *Security of Canada Information Sharing Act* (*SCISA*), enacted in June 2015 as part of the *Anti-Terrorism Act*, *2015* (former Bill C-51) was the GC's first response to address the recommendations made by the O'Connor Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, the findings in the 2004 and 2009 Status Reports of the Auditor General of Canada, the Report of the Standing Committee on Public Accounts concerning those reports, and the recommendations made by the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

In the Fall of 2016, Public Safety Canada (PS) and the Department of Justice Canada (DOJ) held a consultation on potential reforms to Canada's national security framework, including the *SCISA*. Following the subsequent *What We Learned Report*, the PS Minister introduced Bill C-59, also referred to as the *National Security Act, 2017*, in June 2017. The Bill, which received royal assent in June 2019, included amendments to the *SCISA*, which was renamed the *SCIDA*.

> **2000s:** Several incidents and reports highlight national security information sharing challenges in Canada
>
> **2015**: Anti-terrorism Act, 2015 (C-51): Security of Canada Information Sharing Act (SCISA)
>
> **2019**: National Security Act, 2017 (C-59): SCIDA

Overview

The SCIDA establishes an express, stand-alone authority for GC institutions to disclose national security information, including personal information, either proactively or in response to a request, to a core group of 17 designated recipient institutions within the GC that have a recognized national security mandate. 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 *SCIDA* aims to encourage and facilitate effective and responsible information disclosure between GC institutions in order to protect Canada against activities that undermine the security of Canada. As stated in the Act's Preamble, this purpose is to be pursued with a view to respecting the Canadian *Charter of Rights and Freedoms* (*Charter*) and the privacy rights of Canadians under the *Privacy Act* and other federal legislation. Each institution's authority to collect, disclose, retain and use information (including personal information) remains circumscribed by this legal framework. Importantly, the *SCIDA* also does not take precedence over any other statutory or regulatory prohibitions or limitations on the disclosure of information, nor does it 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). The *SCIDA* does not restrict the capacity or discretion of government institutions to disclose information to other government institutions under other existing federal legislation regulating the disclosure of information, such as the *Privacy Act* or specific departmental or program-related legislation.

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 the disclosure prohibited or restricted by other federal legislation or regulations?
3. Is the information being disclosed to one of the 17 designated recipient institutions?
4. Do you believe that the information will contribute to the recipient's national security mandate?
5. Are you satisfied that the disclosure of the information will not affect any person's privacy interest more than is reasonably necessary in the circumstances?
6. Have you provided a statement on the accuracy and reliability of the information as part of your disclosure?
7. Have you created and retained a record of the disclosure prior to disclosing the information?
8. Has your institution provided a record of the disclosure 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), it may be 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, records of the determination and the reasons for it must be retained. 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).

Step 1: Does your institution have information that you believe is linked to an activity that undermines the security of Canada?

Describe how the information to be disclosed is linked to an activity that undermines the security of Canada[1] (**exclude** specific details about any person(s)).

[1] 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.

Type of activities that undermine the security of Canada (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 Explanatory Note for Step 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 that undermines the security of Canada.**

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 or regulations.
- ❑ No, the ability to disclose this information is not prohibited or restricted by other legislation or regulations.

Go to Explanatory Note for Step 2.

Step 3: Is the information being disclosed to one of the 17 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[2]
- ❑ Public Safety Canada
- ❑ Transport Canada
- ❑ Financial Transactions and Reports Analysis Centre of Canada
- ❑ Public Health Agency of Canada
- ❑ Royal Canadian Mounted Police

Go to Explanatory Note for Step 3.

[2] While the Department of National Defence and the Canadian Armed Forces are separate entities, they share the same national security mandate. For each institution's contact details, refer to Appendix G.

Step 4: Do you believe the information will contribute 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 Explanatory Note for Step 4.

Step 5: Are you satisfied that the disclosure of the information will not affect any person's privacy interest more than is reasonably necessary in the circumstances?

Provide a description of how you have satisfied yourself that the disclosure **will not affect any person's privacy interest more than is reasonably necessary in the circumstances**.

> Go to Explanatory Note for Step 5.

Step 6: Have you provided a statement on the accuracy and reliability of the information as part of your disclosure?

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

> Go to Explanatory Note for Step 6.

You should now be prepared to disclose the information!

To assist you in ensuring that all required information is included in the disclosure package, refer to the template disclosure letter in **Appendix C**.

Step 7: Have you created and retained a record of the disclosure prior to disclosing the information?

- ❑ 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 Explanatory Note for Step 7.

Step 8: Has your institution provided a record of the disclosure 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 30th).

Go to Explanatory Note for Step 8.

Guide to the checklist for institutions disclosing information under the SCIDA

> It is important to confirm that your institution is considered a "Government Institution" as defined in section 2 of the SCIDA prior to disclosing any information (refer to **Appendix E**). If your institution does not meet this definition, then it cannot lawfully disclose information under the SCIDA. In such situations, you will need to consider another authority to disclose the required information.
>
> If you are uncertain about whether you meet the legal requirements for any of the following steps or are authorized to disclose information under SCIDA, it is recommended that you consult with your Departmental Legal Services Unit or Access to Information and Privacy (ATIP) Office for advice.

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

- 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 (definition).

- Since the purpose of the Act is to encourage and facilitate the disclosure of information in order to protect Canada's national security interests, this definition is intended to authorize disclosure in support of all federal jurisdiction and responsibilities that involve preventing, as well as addressing, the carrying out of known and new and emerging national security threats.

- The types of activities listed in the SCIDA are illustrative examples of activities that fit within the definition. They are included to give a flavor for the wide range of activities that are considered to be of a level of seriousness and probable extent of impact on Canada to require the recipient institutions to address them under their national security jurisdiction or responsibilities.

- Prior to disclosure, you need to assure yourself that the threshold in the Act is met. This requires you to make the inquiries necessary to ensure that you are satisfied that the

threshold is met before deciding to disclose the information. It may be necessary for you 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 general information to ensure that you may proceed with the disclosure of this information. Refer to **Appendix F** for a description of the designated recipient institutions' national security mandates.

- Informal communication cannot be used in lieu of the formal disclosure process or to replace the formal record-keeping obligations. It is recommended that any 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).

Step 2: Is the disclosure of this information not prohibited or restricted by other federal legislation or regulations?

- The SCIDA provides a standalone authority for the disclosure of information related to the security of Canada where no other explicit authority exists; it does not replace or take precedence over existing statutory or regulatory authorities on the disclosure of information.

- If any other legislation or regulations prohibit the disclosure of the information, then the information may not be disclosed. If any other legislation or regulations impose restrictions or additional requirements to the disclosure of the information, then those 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.

Step 3: Is this information intended for one of the 17 designated recipient institutions?

- To determine whether your institution is authorized to disclose information to another institution under the SCIDA, you must confirm that the intended recipient is one of the federal government institutions designated as recipient institutions under Schedule 3 of the Act. The SCIDA does not authorize the disclosure of information to/from any other level of government or foreign governments.

- While all federal government departments and agencies listed in **Appendix E** can disclose information under the SCIDA, the SCIDA only authorizes the disclosure of information to the heads of a limited number of designated federal government institutions that have jurisdiction or responsibilities that pertain to the security of Canada. The following 17 government institutions have been designated as recipient institutions:

    - Canadian Security Intelligence Service
    - Royal Canadian Mounted Police
    - Canada Border Services Agency
    - Financial Transactions and Reports Analysis Centre of Canada
    - Communications Security Establishment
    - Department of Public Safety and Emergency Preparedness
    - Department of National Defence / Canadian Armed Forces
    - Department of Citizenship and Immigration
    - Department of Transport
    - Department of Foreign Affairs, Trade and Development
    - Canada Revenue Agency
    - Department of Finance
    - Canadian Nuclear Safety Commission
    - Department of Health
    - Canadian Food Inspection Agency
    - Public Health Agency of Canada

- In the event that you are disclosing the same information to more than one designated recipient institution at the same time, you must 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 arrangement (ISA). An ISA can significantly reduce the risk that a given disclosure is unreasonable since it serves as a written understanding of the terms and conditions under which information is shared between institutions, and prevents overbroad or irrelevant disclosures.

- ISAs are useful for establishing common policies, practices and controls by:

    - establishing which specific elements of private information will be disclosed;

    - defining intended purposes and outcomes for the disclosure; and

    - limiting secondary uses and subsequent disclosure.

- ISAs should clearly state that disclosure is always discretionary and should only occur where the disclosing institution is satisfied that all information to be disclosed will contribute to the exercise or carrying out of the recipient's jurisdiction or responsibilities in relation to "activities that undermine the security of Canada". In addition, the ISA should state that the disclosing institution should not disclose information that will affect any person's privacy interest more than is reasonably necessary in the circumstances.

- For more information on preparing an ISA, refer to Treasury Board Secretariat, *Guidance on Preparing Information Sharing Agreements Involving Personal Information*, online:

  https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html.

Step 4: Do you believe that this information will contribute to the recipient's national security mandate?

- In order to strike a balance between furthering the important national security objectives of the SCIDA and respecting the privacy interests of affected individuals, the SCIDA requires that the disclosing institution be satisfied that the disclosed information will "**contribute to**" the exercise of a recipient institution's jurisdiction or responsibilities in respect of "activities that undermine the security of Canada".

- The term "contribute" is not defined in the SCIDA. The ordinary meaning should therefore be used. Contribute is defined as "to lend assistance or aid" or "to have a share in any act or effect…" Note that "contribute" is not preceded by any qualifier (ex.: "significantly", "materially", etc.). Such qualifiers should not, therefore, be read into the Act so as to further limit the disclosure of information contemplated by SCIDA that is not private information. By contrast, disclosure of private information under SCIDA must contribute in a more than trivial or insignificant manner to the recipient institution's exercise of its national security jurisdiction or the carrying out of its responsibilities.

- The wording "will" (contribute) is critical to the SCIDA disclosure threshold. It requires that the link between the information and the recipient's jurisdiction and responsibilities be actual or present, and not merely speculative. Information that is only possibly or potentially or even likely to contribute will not meet the disclosure threshold. Reliability and accuracy are also important factors as, ultimately, information that is seriously flawed is unlikely to contribute to the carrying out of national security functions or jurisdictions.

- Your assessment of the contributive effect of the information will depend on a variety of factors, including the intended recipient institution(s), the nature of its jurisdiction and responsibilities, and the nature of the information to be disclosed. The more a direct link can be traced between the recipient institution's jurisdiction and the nature of the information (including any national security threat that the information tends to reveal), the more likely it is that the disclosure will contribute to the recipient institution's lawful jurisdiction or responsibilities.

- This threshold is not intended to impose a standard of perfection on disclosing institutions, however, it is expected that disclosing institution make **all reasonable efforts** to satisfy themselves that the information will contribute to the recipient institution's national security mandate/responsibilities.

- As described in Step 1, you may need 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 to confirm how it contributes to that institution's national security mandate if uncertain.

- Refer to **Appendix F** for a detailed description of each designated recipient institutions' national security mandate.

Sample Case

The disclosing institution is the Canadian Border Services Agency (CBSA). In performing their statutory duties under the Customs Act and Regulations, customs agents come across information describing ongoing and forthcoming efforts to effect a significant interference with the global information infrastructure, which paragraph 2(g) of the SCIDA identifies as an activity that undermines the security of Canada. The CBSA wishes to disclose this information to the Communications Security Establishment (CSE).

Examining the Communications Security Establishment Act, the CBSA notices that CSE's jurisdiction and responsibilities include the ability to carry out active and defensive cyber operations "on or through the global information infrastructure." While the CBSA may not know, with absolute certainty, whether or not the disclosure will in fact contribute to CSE's jurisdiction or responsibilities, the direct link between the information and CSE's statutory jurisdiction provides a sufficient basis for the CBSA to be "satisfied" that the disclosure will indeed contribute to the exercise of CSE's jurisdiction or responsibilities.

Bulk Disclosures (Sharing Large Amounts of Data)

The SCIDA may authorize institutions to disclose data other than on a case-by-case basis where all SCIDA requirements are met (including for datasets or other specific categories of information). In order to ensure that a disclosure is authorized, it is important that **every piece of information in the bulk disclosure or category meets the requirements for disclosure set out in section 5 of the SCIDA**.

As there is greater risk with regards to the misuse or mislabeling of information when shared in bulk, federal institutions should put robust frameworks in place for sharing of this type of bulk data to satisfy themselves that all requirements of the Act have been met, including using precise caveats and statements of accuracy and reliability. When responding to requests for information for bulk datasets, institutions should minimize the sharing of extraneous data whenever possible.

The scope of any bulk disclosure needs to be closely tailored to the recipient's national security jurisdiction or responsibilities, and where it forms part of a routine process, should be reviewed at regular intervals to ensure continued compliance with the requirements of the SCIDA.

Institutions must ensure that records kept for bulk disclosures include an appropriately robust description of the information relied upon to satisfy themselves that the disclosure of all elements of the information meets section 5 of the Act (including how the disclosure contributes to the recipient's national security mandate) and that the level of internal oversight is commensurate with the privacy risk.

Step 5: Are you satisfied that the disclosure of the information will not affect any person's privacy interest more than is reasonably necessary in the circumstances?

- Before information can be disclosed under the SCIDA, you must also be satisfied that the disclosure will not impact a person's privacy interests (including any third parties) any more than is reasonably necessary in the circumstances. Any information that will impact a person's privacy interests more than reasonably necessary in the circumstances must be removed before the disclosure takes place.

- Whether the impact on a person's privacy interest is considered "reasonably necessary" will depend on the various factors and the particular circumstances of each case. Relevant considerations may include contextual factors such as the type and nature of the information in question, the purpose for initially collecting this information and the particular purpose for the disclosure in the circumstances.

- To "satisfy" yourself that this threshold has been met, you must to make meaningful efforts to minimize the potential impact the disclosure may have on any person's privacy interests (e.g. remove any non-essential personal information and ensure that only the information that most effectively advances the particular purpose of the disclosure is included). You can further address the impact on privacy interests flowing from the disclosure by placing limitations (caveats) on further use or sharing.

- Establishing an early dialogue with the designated recipient institution will assist you in determining how to minimize the impact on any person's privacy interests while still contributing to the recipient's national security mandate.

- **It is important to remember that this threshold is intended to help determine the scope of what can be disclosed**, and **not** whether the disclosure should occur. While a disclosing institution should aim to disclose the least amount of private information possible to achieve the purpose of the disclosure, this step should not prevent you from disclosing necessary/crucial elements of information that you believe will contribute to the exercise of another institution's NS jurisdiction or the carrying out of its responsibilities.

- "Privacy interests" in the context of the SCIDA encompass the interests of both natural persons and corporations. Such interests include sensitive or proprietary information about corporations as well as any identifiable information about an individual, such as, name, age, marital status, race, national or ethnic origin, religion, education, address, fingerprints, blood type, and medical, criminal, or employment history.

- The degree to which information may affect the privacy interest of any person is a function of the information itself and of what it may tend to reveal. For instance, although an I.P. address may not appear private on its face, it may reveal an individual's web

Privacy Considerations

- Possible future (subsequent) disclosures should be a factor in assessing what information can or should be disclosed to a recipient institution. As the SCIDA does not govern or limit any subsequent disclosures of information, such an assessment should also inform the content of caveats, which can help disclosing institutions limit the impact of a disclosure on privacy interests. For example, disclosing institutions may include caveats such as: "The information is prohibited from further distribution, without prior written consent of [the disclosing institution]" or "the information must be destroyed after [a set period of time]."

- Subsequent uses of personal information continue to be governed by generally applicable laws such as the Charter and the Privacy Act, and in some cases more specific confidentiality obligations such as in the Income *Tax Act* and the *Customs Act*.

- Respect for caveats and originator control is a guiding principle of the SCIDA and caveats should be followed in all circumstances, except where further disclosure is required by law or exigent circumstances would make it impracticable or unfeasible to follow (i.e. threat is imminent).

browsing history, which would in turn reveal intimate details of the individual's lifestyle and personal choices.

- If your institution expects to disclose personal information under the SCIDA, you should consider whether a formal assessment of its associated privacy impacts is warranted, and whether a new or updated privacy impact assessment (PIA) is needed. 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, may constitute a substantial modification to an institution's regular programs or activities in certain circumstances, 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.

Step 6: Have you provided a statement on the accuracy and reliability of the information as part of your disclosure?

- 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.
- The purpose of this provision is twofold: to help the disclosing institution in exercising their discretion as to whether or not certain information should be disclosed under SCIDA by reminding them to consider these factors and to help the recipient institution determine whether the information can/should be used (and under what conditions), whether it needs to be corroborated, and how much weight should be attributed to it.
- In preparing the statement of accuracy and reliability, you should make every reasonable effort to ensure that the information is as accurate, complete and as up-to-date as possible. This is key to responsible and effective disclosures. **Formulaic (templated)**

language should be avoided, unless the nature and source of information disclosed is derived from a routine process.

- Any concerns regarding the accuracy of the information or reliability of the manner in which it 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?
    - 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?
- Of course, disclosing institutions may not always be in possession of information allowing for an assessment of the accuracy of the information to be disclosed, or of the reliability of the manner by which it was obtained. In such circumstances, you will still need to provide this statement to the recipient institution and clearly highlight the

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 been made or requested in relation to personal information should be included as part of the statement of accuracy.

limitations preventing you from making a full assessment as to reliability or accuracy. Any other concerns as to reliability or accuracy should also be flagged in the statement.

You should now be prepared to disclose the information!

To assist you in ensuring that all required information is included in the disclosure package, refer to the template disclosure letter in **Appendix C**.

Step 7: Have you created and retained a record of the disclosure prior to disclosing the information?

- The SCIDA re quires that a complete set of records of disclosures and receipts under the Act is created and maintained, and made available for review by the National Security Intelligence Review Agency (NSIRA) each year. This requirement is intended to standardize record keeping across government institutions and increasing accountability and transparency with respect to the information disclosure practices authorized by the SCIDA.

- In order to keep appropriate records, 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 and will facilitate any follow-ups that may be needed between the disclosing and recipient institutions.

- If your institution chooses not to use the record-keeping template, you **must** still ensure that your institution keeps, at a minimum, a record of the following information:

    - a description of the disclosed information;

    - the name of the individual who authorized its disclosure;

    - the name of the recipient institution;

    - the date on which the information was disclosed;

    - a description of the information that was relied on to satisfy you that the disclosure was authorized under the SCIDA; and,

    - any other information specified by the regulations (**this requirement is currently not applicable as no regulations in place**).

- Of note, you must ensure that the record includes **an appropriately robust description of the information you relied upon to satisfy yourself that the disclosure meets section 5 of the SCIDA** (including sufficient detail on how the disclosure will contribute to the recipient's national security mandate and will not affect any person's privacy interests more than reasonably necessary in the circumstances).

- Likewise, as information may only be disclosed under the SCIDA to the head of a designated recipient institution or persons who have been designated by the head to receive information under the SCIDA, you must ensure to include information about the person who authorized the disclosure and who received the information for each disclosure, unless the disclosure of that information would result in a risk to an ongoing investigation or to whoever is disclosing/receiving the information.

- For a list of heads of institutions and designated persons authorized to receive information under the SCIDA, as well as departmental contact information, refer to **Appendix G**.

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

Step 8: Has your institution provided a record of the disclosure to the National Security and Intelligence Review Agency (NSIRA)?

- A copy of each record of disclosure produced by a disclosing institution must be retained and provided to the National Security and Intelligence Review Agency (NSIRA) by January 30th of each year (for the previous calendar year).

- The NSIRA will then prepare a report on the information disclosure practices undertaken by the GC pursuant to the SCIDA during the previous calendar year. The report is presented to and tabled in Parliament by the Minister of Public Safety.

- This oversight mechanism plays a crucial transparency and accountability function for the information disclosure practices authorized under the SCIDA.

Steps for institutions receiving information under the SCIDA

Key Questions for Recipient Institutions

1. Has your institution received information under the SCIDA?
2. Which Government of Canada institution disclosed this information to you?
3. Which designated individual within your institution received the information?
4. Does the disclosure contain any unnecessary personal information?
5. Have you created and retained a record of the receipt?
6. Has your institution provided a record of the receipt 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 must create and retain a record of the receipt. A record-keeping template for institutions receiving 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 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).

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

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 Explanatory Note for Step 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 that undermines the security of Canada.**

Step 2: Which institution disclosed this information to your institution?

This information was disclosed by the following:

Name of Institution: _____

> Go to Explanatory Note for Step 2.

Step 3: Which designated individual within your institution received the information?

This information was received by the following:

- ❑ Head of the institution

  OR

- ❑ Designated person

Name/Position: _____

Branch/Division: _____

Date of receipt (mm/dd/yyyy): _____

> Go to Explanatory Note for Step 3.

Step 4: Does the disclosure contain any unnecessary personal information?

- ❑ No. I am satisfied that all personal information disclosed to my institution is necessary for my institution to carry out its national security mandate and/or responsibilities.

  OR

- ❑ No. The disclosure did not contain any personal information.

  OR

- ❑ Yes, the disclosure contains some personal information that it is not necessary for my institution to carry out its national security mandate, however, that information has been destroyed or returned to the disclosing institution.

  OR

- ❑ Yes, the disclosure contains some personal information that it is not necessary for my institution to carry out its national security mandate, however, the retention of the information is required by law or because it relates to the performance of Canadian Security Intelligence Service (CSIS) duties and functions under section 12 of the Canadian Security Intelligence Service Act.

Go to Explanatory Note for Step 4.

Note 5: 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: Have you created and retained a record of the 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 Explanatory Note for Step 5.

Step 6: Has your institution provided a record of the receipt 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 30th).

Go to Explanatory Note for Step 6.

Guide to the checklist for institutions receiving information under the SCIDA

> It is important to confirm that your institution is one of the designated recipients in Schedule 3 of the SCIDA prior to accepting a disclosure of information (refer to **Appendix F**). If your institution is not listed, it cannot lawfully receive information under the SCIDA. In such situations, you will need to consider another authority to obtain the required information.
>
> If you are uncertain about whether you meet the legal requirements for any of the following steps or are authorized to disclose information under SCIDA, it is recommended that you consult with your Departmental Legal Services Unit or Access to Information and Privacy (ATIP) Office for advice.

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

- 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 (definition).

- Since the purpose of the Act is to encourage and facilitate the disclosure of information in order to protect Canada's national security interests, this definition of is intended to authorize disclosure in support of all federal jurisdiction and responsibilities that involve preventing, as well as addressing, the carrying out of known and new and emerging national security threats.

- The types of activities listed in the SCIDA are illustrative examples of activities that fit this 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 the event that you have requested information from a disclosing institution, it is 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, however, 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.

- If requesting information from an institution not listed in Schedule 3 of the SCIDA or an institution that discloses infrequently, it is recommended that you encourage the disclosing institution to consult their Legal Services Unit and/or Public Safety Canada to ensure they are fully informed of their legal obligations with respect to disclosing information under the SCIDA. You should also ensure that your request clearly indicates that the request itself does not constitute or confer authority for the other institution to disclose personal information (see **Appendix B** for sample request letter).

- In the event that you have received a proactive disclosure, some of the preliminary steps in this checklist may not apply. Nevertheless, you must keep a record of the basic information required under Step 5, including 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. You must also ensure that any personal information included in the disclosure is appropriate and is properly handled, as described in the explanatory note to **Step 4**.

Step 2: Which institution disclosed this information to your institution?

- By default, the definition of a government institution under SCIDA covers virtually all federal departments, agencies and Crown corporations, as well as parent Crown corporations and wholly owned subsidiaries. However, it is a good practice to ensure that the institution disclosing the information to you is considered a Government Institution, as defined in section 2 of the Act, before accepting receipt of a disclosure. The SCIDA does not authorize the disclosure of information to/from other levels of government or foreign governments.

- To verify whether the disclosing institution is a Government of Canada institution authorized to disclose information under the SCIDA, refer to **Appendix E**.

- As set out in the explanatory note to **Step 5**, you must keep a record of which institution disclosed the information to you.

Privacy Considerations

- If your institution is likely to receive information from other departments and agencies on a regular basis, it may be beneficial to develop an information sharing agreement (ISA) to govern this relationship – and protect any personal information.
    - ISAs are useful for establishing common policies, practices and controls by:
    - establishing which specific elements of personal information will be disclosed;
    - defining intended purposes and outcomes for the disclosure; and,
    - limiting secondary uses and onward transfer.
- ISAs should clearly state that disclosure is always discretionary and should only occur where the disclosing institution is satisfied that all information to be disclosed will contribute to the exercise or carrying out of the recipient's jurisdiction or responsibilities in relation to "activities that undermine the security of Canada". In addition, the ISA should state that the disclosing institution should not disclose information that will affect any person's privacy interest more than is reasonably necessary in the circumstances.
- For more information on preparing an ISA, refer to Treasury Board Secretariat, "Guidance on Preparing Information Sharing Agreements Involving Personal Information", online:

  https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html.

Step 3: Which designated individual within your institution received the information?

- Under the SCIDA, information may only be disclosed to the head of a designated recipient institution or to persons who have been designated the authority to receive

information under SCIDA. This requirement is to ensure that only those who require the information to fulfill their mandate receive the information.

- To verify whom within your institution has been designated as a person authorized to receive information under the SCIDA, refer to **Appendix G**. If you are uncertain as to the designation of any person(s), it is strongly recommended that you consult with your Departmental Legal Services Unit before proceeding to ensure the proper designations are in place.

- If the head of an institution wishes for other designated persons to exercise the functions contemplated in the SCIDA, a formal designation should be put in place. A disclosure will not be authorized by the SCIDA if information is disclosed to anyone other than the head, or their designate, even if the recipient is listed in Schedule 3 of the SCIDA.

Step 4: Does this information include any personal information?

- 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 exercise its national security jurisdiction, or to carry out its responsibilities, 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;

    - CSIS, if the information is relevant to the performance of its duties under s. 12 of the *Canadian Security Intelligence Service Act*; and,

    - Any instance where a Litigation Hold is in place.

- As described in the explanatory note to **Step 1**, you are encouraged to communicate with the disclosing institution prior to a disclosure so that they understand why the 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.

- "Personal information" in the context of the SCIDA includes sensitive or proprietary information about a person (including corporations) that, if publicly disclosed, may affect their privacy interests. It includes any identifiable information about an individual, such as, 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 is considered personal information, refer to section 3 of the *Privacy Act*[3]).

Privacy Considerations

- As the SCIDA does not govern or limit any subsequent disclosures or use of information, disclosing institutions may impose certain caveats limiting how a recipient institution deals with the personal information once it is received.

- Respect for caveats and originator control is a guiding principle of the SCIDA, and caveats should be followed in all circumstances, except where further disclosure is required by law or exigent circumstances would make it impracticable or unfeasible to follow (i.e. threat is imminent).

Step 5: Have you created and retained a record of the receipt?

- The SCIDA re quires that a complete set of records of disclosures and receipts under the Act is created and maintained, and made available for review by the National Security Intelligence Review Agency (NSIRA) each year. This requirement is intended to standardize record keeping across government institutions and increasing accountability and transparency with respect to the information disclosure practices authorized by the SCIDA.

[3] https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html

- In order to keep appropriate records, 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 and will facilitate any follow-ups that may be needed between the disclosing and recipient institutions.

- If your institution chooses not to use the record-keeping template, you **must** still ensure that your institution keeps, at a minimum, a record of 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 (**this requirement is currently not applicable as no regulations in place**).

> **Note**: It is important to remember to complete a record of disclosure for each disclosure received and provide a copy of it to the appropriate person within your institution so that it can be retained for annual reporting purposes. **A standardized process for record keeping is highly recommended for all recipient institutions receiving information under the SCIDA**.

Step 6: Has your institution provided a record of the receipt to the National Security and Intelligence Review Agency (NSIRA)?

- A record of each receipt of information must be retained and provided to the National Security and Intelligence Review Agency (NSIRA) by January 30th of each year (for the previous calendar year).

- The NSIRA will then prepare a report on the information disclosure practices undertaken pursuant to the SCIDA during the previous calendar year. The report is presented to and later tabled in Parliament by the Minister of Public Safety Canada.
- This oversight mechanism plays a crucial transparency and accountability function for the information disclosure practices authorized under the SCIDA.

Appendix A

Record-keeping template for institutions disclosing and receiving 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 30th. Completing this template for each disclosure will help you meet the record-keeping obligations for disclosing and recipient institutions under the SCIDA.

A Disclosure of information under the *SCIDA* **(To be completed by disclosing institution)**	
Name of Disclosing Institution:	
Name of Individual Authorizing Disclosure:	**Position of Individual Authorizing Disclosure:**
File Reference Number:	
Description of Information (attach annex if more space is required):	
Name of Recipient Institution:	
Name of Designated Person (Recipient):	**Position of Designated Person (Recipient):**
Rationale for Disclosure (attach annex if more space is required):	
Date of Disclosure:	

B **Receipt of information under the *SCIDA* (To be completed by recipient institution)**

Name of Recipient Institution:

Name of Individual Receiving Information:	**Position of Individual Receiving Information:**

File Reference Number:

Name and Position of Individual Authorizing Disclosure:

Was the information received from the same individual listed in Section A?

☐ Yes ☐ No

If no, provide the name, position and institution of the individual that disclosed the information:

Description of Information:

Is the description of the information above in Section A what was received by your institution?

☐ Yes ☐ No

If no, provide a full description of the information received (attach annex if more space is required):

Date of Receipt:

Return or Destruction of Personal Information:

Was any personal information returned to the disclosing institution or destroyed?

☐ Yes ☐ No

If yes, specify what information was returned or destroyed and provide the date when this occurred:

Appendix B
SCIDA request letter (template)

Name of individual or unit/division/branch
Recipient institution
Address

Name of individual or unit/division/branch
Disclosing institution
Address

Date

RE: Request for a Disclosure of Information under the *SCIDA*

Dear individual or unit/division/branch,

Recipient institution kindly requests the disclosure of information, which your institution may have in its possession, relating to the following subject:

- Describe the information being requested.

Recipient institution is designated as a Government of Canada institution authorized to receive information under the *Security of Canada Information Disclosure Act* (*SCIDA*) and considers that information related to the above-noted subject will contribute to its jurisdiction and responsibilities in respect of an activity that may undermine the security of Canada, specifically as it relates to type of activity.

Further describe how this information will contribute to the exercise of your institution's jurisdiction and/or the carrying out of its responsibilities as it relates to this activity (e.g. detection, identification, analysis, prevention, investigation or disruption of activities that undermine the security of Canada).

[For use if disclosing institution is not listed in Schedule 3 of SCIDA.] Please note that this request is being provided to assist you in making a determination to disclose the requested information. It does not constitute or confer authority for you to disclose the information, nor does it waive any requirements of the *SCIDA* that you may be subject to as a disclosing

institution (including record-keeping requirements). For questions about the *SCIDA*, we recommend you communicate with Public Safety Canada at scci-ccsi@ps-sp.gc.ca.

If you have any questions or concerns related to this request, please do not hesitate to contact me [or add another contact person] at [telephone number].

Thank you,

Name of individual and/or unit/division/branch disclosing the information

Appendix C
SCIDA disclosure letter (template)

File Reference Number: #### / XXXX / XXXX / ####

Name of individual or unit/division/branch
Disclosing institution
Address

Name of individual or unit/division/branch
Recipient institution
Address of recipient institution

Date

RE: *SCIDA* Disclosure of Information

Dear individual or unit/division/branch,

[Remove if proactive disclosure: This letter is in response to your request dated on Click here to enter a date.]

Disclosing institution name is disclosing the attached information to Recipient institution pursuant to section 5 (1) of the *Security of Canada Information Disclosure Act* (*SCIDA*).

Our institution has information that we believe will contribute to your institution's jurisdiction and responsibilities with respect to an activity that undermines the security of Canada, specifically as it relates to type of activity.

Describe the recipient institution's national security jurisdiction and/or responsibilities as it relates to this activity (e.g. detection, identification, analysis, prevention, investigation or disruption of activities that undermine the security of Canada).

You may only disclose this information in accordance with the following caveat(s):

- List any caveats on the disclosed information here.

Provide a statement on the accuracy of the information to be disclosed and the reliability of the manner in which the information was obtained.

If you have any questions or concerns related to this disclosure, please do not hesitate to contact me [or add another contact person] at [telephone number].

Thank you,

Name of individual and/or unit/division/branch disclosing the information

Appendix D

File reference numbering system

For every disclosure of information under the *Security of Canada Information Disclosure Act* (*SCIDA)*, it is recommended that the disclosing institution generate a File Reference Number to be used by both the disclosing and recipient institutions for record-keeping and external reporting purposes, e.g. annual report to the National Security and Intelligence Review Agency (NSIRA).

We recommend that a File Reference Number be composed of at least the following four parts:

Year /	**Disclosing Institution /**	**Recipient Institution /**	**Unique Identifier Number**
e.g.: 2022	(Acronym) e.g.: CBSA	(Acronym) e.g.: IRCC	e.g.: 0001 **A unique identifier number should be assigned by the disclosing institution and used by both the disclosing and recipient institution for each disclosure of information.*

*For institutions that are comprised of several **branches or regional offices** that may disclose or receive information for national security purposes under the SCIDA, it is recommended that the institution add an additional descriptor to its acronym in the File Reference Number (e.g. CBSA-QUE). Doing so will ensure that SCIDA records are more easily discernible and will facilitate cross-referencing activities and reporting on disclosures.

As an example, a File Reference Number for a disclosure of information by the Canada Border Services Agency's Quebec Intelligence Operations Division to Immigration, Refugees and Citizenship Canada could appear as follows:

FILE REFERENCE NUMBER: 2022 / CBSA-QUE / IRCC / 0001

Appendix E

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 Council3 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 F
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 statues 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 (GC). 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 GC 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 GC 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 GC, 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 GC (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 CSE 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 CSE 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 analyse 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].

During the pre-defined period specific to each case where CSE operates under the Assistance mandate, 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. CSE has rigorous internal monitoring of all mandated 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 CSE 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, analysing, retaining or disclosing publicly available information;
- Acquiring, using, analysing, 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 Taliban, ISIL (Da'esh) and Al-Qaida.

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, Canadas' 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.

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.

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.

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 Ac*t, 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 Harbouring [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 G

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

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

Canadian Food Inspection Agency

Head:

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

Person Designated by the Head:

- VP and Chief Security Office Corporate Management Branch
  Email: cfia.vpcmb-vpdggi.acia@inspection.gc.ca

- VP Policy and Programs Branch
  Email: cfia.vppolicyprograms-vppolitiquesetprogrammes.acia@inspection.gc.ca

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: cnsc.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

Communications Security Establishment

Head:

- Chief of the Communications Security Establishment

Person Designated by the Head:

- Director, Operational Policy

- For proactive disclosures, please contact:
  Email: 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, Security and Exceptional Cases Division
- Case Management Branch
  Email: 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:

- Executive Director, Intelligence Policy and Programs Division
  Unclassified Email: SCIDA-LCISC@international.gc.ca
  Classified Secret Email: SCIDA-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

- Executive Assistant to ADM:
  Telephone: 613-946-6700

- Director of ADMO:
  Telephone: 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
  Classified Email: CFINTCOM_RDCO@spartan.mil.ic.ca

- Canadian Forces Integrated Command Centre (24/7)
  Telephone: 613-998-4136
  Unclassified Email: cficc@forces.gc.ca
  Classified Email: cficc-ccifc@forces.cmil.ca

Department of Public Safety and Emergency Preparedness Canada

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

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

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:

- The Assistant Commissioner of Federal Policing National Security and Protective Policing
- The Director General, Federal Policing National Security
  Email (unclassified): ACC-NOC@rcmp-grc.gc.ca
  Email (classified): RCMP-GRC.C5@c.international.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). The Commissioner has designated 2 designated officials to receive information under the SCIDA, namely the Assistant Commissioner of Federal Policing National Security and Protective Policing and the Director General, Federal Policing National Security. Disclosures to the RCMP must be addressed to the Commissioner or a designated official, and routed through the point of contact provided above.

Appendix H

Security of Canada Information Disclosure Act (SCIDA)

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

Assented to 2015-06-18

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

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

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;

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

- 2015, c. 20, s. 2 “Preamble”
- 2019, c. 13, s. 113

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

(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 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 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

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.

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.

SCHEDULE 1 (Section 2 and subsection 10(2))

Excluded Institutions

SCHEDULE 2 (Section 2 and subsection 10(2))

Additional Institutions

- 2015, c. 20, s. 2 “Sch. 2”
- 2019, c. 13, s. 73

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

Recipient Government of Canada Institutions and Their Heads

Column 1	Column 2
Recipient Institution	Head
• Canada Border Services Agency *Agence des services frontaliers du Canada*	President of the Canada Border Services Agency
• Canada Revenue Agency *Agence du revenu du Canada*	Commissioner of Revenue
• Canadian Armed Forces *Forces armées canadiennes*	Chief of the Defence Staff
• Canadian Food Inspection Agency *Agence canadienne d'inspection des aliments*	President of the Canadian Food Inspection Agency
• Canadian Nuclear Safety Commission *Commission canadienne de sûreté nucléaire*	President of the Canadian Nuclear Safety Commission

• Canadian Security Intelligence Service *Service canadien du renseignement de sécurité*	Director of the Canadian Security Intelligence Service
• Communications Security Establishment *Centre de la sécurité des télécommunications*	Chief of the Communications Security Establishment
• Department of Citizenship and Immigration *Ministère de la Citoyenneté et de l'Immigration*	Minister of Citizenship and Immigration
• Department of Finance *Ministère des Finances*	Minister of Finance
• Department of Foreign Affairs, Trade and Development *Ministère des Affaires étrangères, du Commerce et du Développement*	Minister of Foreign Affairs
• Department of Health *Ministère de la Santé*	Minister of Health
• Department of National Defence *Ministère de la Défense nationale*	Minister of National Defence

• Department of Public Safety and Emergency Preparedness *Ministère de la Sécurité publique et de la Protection civile*	Minister of Public Safety and Emergency Preparedness
• Department of Transport *Ministère des Transports*	Minister of Transport
• Financial Transactions and Reports Analysis Centre of Canada *Centre d'analyse des opérations et déclarations financières du Canada*	Director of the Financial Transactions and Reports Analysis Centre of Canada
• Public Health Agency of Canada *Agence de la santé publique du Canada*	President of the Public Health Agency of Canada
• Royal Canadian Mounted Police *Gendarmerie royale du Canada*	Commissioner of the Royal Canadian Mounted Police

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