LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

LEGISLATIVE SUMMARY

BILL C-59:
AN ACT RESPECTING NATIONAL SECURITY MATTERS

Publication No. 42-1-C59-E
3 June 2019

Tanya Dupuis
Chloé Forget
Holly Porteous
Dominique Valiquet
Legal and Social Affairs Division
Parliamentary Information and Research Service

Library of Parliament ***Legislative Summaries*** summarize bills currently before Parliament and provide background about them in an objective and impartial manner. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations. Legislative Summaries are revised as needed to reflect amendments made to bills as they move through the legislative process.

Notice: For clarity of exposition, the legislative proposals set out in the bill described in this Legislative Summary are stated as if they had already been adopted or were in force. It is important to note, however, that bills may be amended during their consideration by the House of Commons and Senate, and have no force or effect unless and until they are passed by both houses of Parliament, receive Royal Assent, and come into force.

Any substantive changes in this Legislative Summary that have been made since the preceding issue are indicated in **bold print**.

Legislative Summary of Bill C-59
(Legislative Summary)

Publication No. 42-1-C59-E

Ce document est également publié en français.

CONTENTS

LEGISLATIVE SUMMARY OF BILL C-59: AN ACT RESPECTING NATIONAL SECURITY MATTERS

1 BACKGROUND

On 20 June 2017, the Minister of Public Safety and Emergency Preparedness, tabled Bill C-59, An Act respecting national security matters (short title: National Security Act, 2017) in the House of Commons.[1]

Bill C-59 is the culmination of a long series of events, commissions of inquiry, public consultations and legislative measures respecting terrorism and national security, including but not limited to, in chronological order:

- 1977–1981: Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (McDonald Commission);[2]
- 1984: In response to the recommendations of the McDonald Commission, creation of a civilian intelligence service (Canadian Security Intelligence Service) to replace the Royal Canadian Mounted Police National Security Service;
- 1985: Bombing of Air India flight 182;
- 2001: *Anti-terrorism Act* adopted following September 11 attacks in the United States;
- 2006: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (O'Connor commission);[3]
- 2008: Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin (Iacobbuci commission);[4]
- 2010: Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (Major commission);[5]
- 2014: Terrorist attacks in Ottawa and in Saint-Jean-sur-Richelieu, Quebec;
- 2015: *Anti-terrorism Act, 2015* (Bill C-51) adopted;[6]
- 2016: Government consultations on *Our Security, Our Rights: National Security Green Paper, 2016*;[7]
- 2017: Report on the consultations: *National Security Consultations: What We Learned Report*;[8] and
- 2017: Adoption of the *National Security and Intelligence Committee of Parliamentarians Act* (Bill C-22).[9]

1.1 PURPOSE AND KEY AMENDMENTS OF BILL C-59

Bill C-59 can be considered "major" national security legislation for at least two reasons:

- it creates a comprehensive system for reviewing national security activities (in contrast to the current fragmentary system) to act as a counterweight both to the powers of the intelligence agencies and to the application of the *Anti-terrorism Act*, which has been expanded since 2001; and
- it amends certain aspects of the former Bill C-51 (*Anti-terrorism Act, 2015*), which some believe violates the *Canadian Charter of Rights and Freedoms*.[10]

Bill C-59 is divided into 11 parts:

- Parts 1 and 2 of the bill create, respectively, new federal institutions responsible for reviewing national security activities: the National Security and Intelligence Review Agency (clauses 2 to 49) and the Intelligence Commissioner (clauses 50 to 75).
- Part 1.1 of the bill creates the Avoiding Complicity in Mistreatment by Foreign Entities Act (clauses 49.1 and 49.2).
- Parts 3 and 4 of the bill concern, respectively, two of the main intelligence agencies: the Communications Security Establishment and the Canadian Security Intelligence Service (clauses 76 to 111).
- Parts 5 and 6 of the bill more fully regulate information-sharing practices employed, respectively, between federal institutions and by those maintaining the "no fly" list provided for in the *Anti-terrorism Act, 2015* (clauses 112 to 139).
- Parts 7 and 8 of the bill are designed, respectively, to tighten special terrorist prevention practices and to ensure that adequate protection measures are applied for adolescent suspects (clauses 140 to 167).
- Part 9 (clause 168) of the bill provides for a parliamentary review of Bill C-59 after five years, if possible in parallel with the review of the *National Security and Intelligence Committee of Parliamentarians Act*.
- Part 10 of the bill (clauses 169 to 173) provides for the coming into force of Bill C-59.

2 DESCRIPTION AND ANALYSIS

2.1 PART 1: ENACTMENT OF THE NATIONAL SECURITY AND INTELLIGENCE REVIEW AGENCY ACT (CLAUSES 2 TO 49)

Part 1 of the bill enacts An Act to establish the National Security and Intelligence Review Agency (short title: National Security and Intelligence Review Agency Act [NSIRA Act]) to create the National Security and Intelligence Review Agency (NSIRA), which is roughly modelled on the Security Intelligence Review Committee (SIRC), the body currently mandated to review the lawfulness of the activities of the Canadian Security Intelligence Service (CSIS).

Section 3 of the NSIRA Act provides for a minimum of four and a maximum of seven NSIRA members, including its chair. Section 4 provides that NSIRA members are to be appointed by the Governor in Council and that the members will serve for a five-year term, with the possibility of being reappointed for a maximum of five additional years, and may only be removed for cause. Section 4(7) of the NSIRA Act specifies that the chair and vice-chair may be designated to serve on either a full- or part-time basis.

Sections 6(1) and 6(2) of the NSIRA Act stipulate that the Governor in Council must act in accordance with Treasury Board directives in establishing pay and compensation.

Sections 49 and 50 of the NSIRA Act require, respectively, that NSIRA members swear an oath or solemn confirmation and that they maintain a Government of Canada security clearance. Changes to the *Security of Information Act* (SOIA)[11] under clause 35 of the bill suggest that former and currently serving NSIRA members will be permanently bound to secrecy under the SOIA, which suggests that they and employees of the NSIRA's secretariat will be privy to special operational information that identifies security and intelligence sources and methods.

Sections 41 to 48 of the NSIRA Act set out provisions for a secretariat to support the NSIRA's work.

2.1.1 The National Security and Intelligence Review Agency Mandate

The NSIRA's remit under section 8 of the NSIRA Act is broad, empowering the Agency to review and make findings and recommendations not only on the lawfulness but also on the reasonableness and necessity of all national security and intelligence activities undertaken by CSIS, the Communications Security Establishment (CSE) and any federal department or that a minister refers to the NSIRA. Section 8(3) specifies that the NSIRA may make findings and recommendations on compliance with the law and any applicable ministerial direction, as well as on the reasonableness and necessity of a department's exercise of its powers.

To ensure clarity about the scope of the NSIRA's mandate, section 7.1 indicates that the Agency may determine the procedure to be followed in the exercise of its powers or the performance of any of its duties or functions.

As the transitional provisions in clauses 3 to 17 of the bill indicate, the proposed NSIRA will lead to the elimination of both SIRC and the Office of the Communications Security Establishment Commissioner (OCSEC), the latter of which currently provides lawfulness review of CSE activities.

2.1.2 A Bifurcated Information Access Regime

Section 11 of the NSIRA Act indicates that, for the purposes of both review and complaints investigations, the NSIRA is entitled to receive from departmental deputy heads or employees "any documents and explanations that the Agency deems necessary for the exercise of its powers and the performance of its duties and functions."

At the same time, Bill C-59 creates two different information access regimes for the NSIRA, one for its review work and another for its investigation of complaints.

2.1.2.1 Reviews

Section 8(2.1) of the NSIRA Act requires the NSIRA to review the implementation of significant aspects of every new or modified ministerial directive issued to CSIS, CSE or any other department if the directive relates to national security or intelligence.

Section 9 of the NSIRA Act addresses information access in relation to NSIRA review work. With the exception of Cabinet confidences, the NSIRA will have broad and timely access to information, including information that is protected by solicitor–client privilege, professional secrecy of advocates and notaries, or litigation privilege. In referring to "information in the possession" of any department, section 9(1) provides the NSIRA with right of access to third-party information and intelligence, such as intelligence shared by foreign allies.[12]

It is worth noting that the proposed NSIRA authorities related to the Agency's review function are more limited than those held by the CSE Commissioner, who, under section 273.63(4) of the *National Defence Act*,[13] had all the powers of a commissioner under Part II of the *Inquiries Act*[14] in carrying out his or her duties. This diminution of authorities has implications with respect to the conditions under which the NSIRA accesses information.

Whereas SIRC and OCSEC reported their review findings to the Minister of Public Safety and Emergency Preparedness and the Minister of National Defence, respectively, the NSIRA is to report to "a federal minister" responsible for the Agency, as designated by the Governor in Council under section 55 of the NSIRA Act.

2.1.2.2 Investigations

Under section 8 of the NSIRA Act, the NSIRA will take over SIRC's and OCSEC's responsibilities for investigation of complaints about CSIS and CSE activities, including whistle-blower complaints involving special operational information and complaints about CSIS's advice to deputy heads concerning individual security clearances and threat assessments related to citizenship applications. The NSIRA will also take over complaints made in relation to the national security activities of the Royal Canadian Mounted Police (RCMP). The distinction between complaints to be investigated by the Civilian Review and Complaints Commission for the RCMP and complaints to be investigated by the NSIRA will be achieved through amendments to the *Royal Canadian Mounted Police Act*,[15] under clauses 41 to 43 of Bill C-59.

Section 10 of the NSIRA Act creates a separate information access regime for the NSIRA in relation to its complaints investigation role. In relation to the investigation of a complaint, section 27 of the NSIRA Act empowers the NSIRA both to compel persons before the Agency to provide written or oral evidence under oath and "to receive and accept the evidence and other information, whether on oath or by affidavit or otherwise, that the Agency considers appropriate, whether or not that evidence or information is or would be admissible in a court of law."

Of note, section 10 limits the NSIRA's access to information in the possession or under the control of only three agencies: CSIS, CSE and the RCMP.

With respect to departmental investigations, section 7 of the *Inquiries Act* empowers an inquiry commissioner to "enter into and remain within any public office or institution"; "have access to every part thereof"; "examine all papers, documents, vouchers, records and books of every kind belonging to the public office or institution"; and to summon and administer oaths to persons giving oral and written evidence. Section 8 of the *Inquiries Act* empowers a commissioner to subpoena a person to appear to provide testimony and provide documentation.

To avoid unnecessary duplication, section 15.1(1) of the NSIRA permits the NSIRA to coordinate its activities with the compliance investigations of the Privacy Commissioner of Canada under section 37(1) of the *Privacy Act*.[16] For the purposes of coordination, the NSIRA is also permitted to share information with the Privacy Commissioner about the Agency's section 8 reviews.

Section 27.1 obliges the NSIRA to suspend an investigation if, after consultation with the appropriate department, the Agency considers that continuing the investigation would compromise or seriously hinder an ongoing criminal investigation or proceeding.

Section 52(1) stipulates that, to avoid disclosure of confidential information, the NSIRA must consult with implicated deputy heads in preparing statements to complainants or reports on denied security clearances or citizenship applications. It is unclear how any disputes concerning the redaction of these or the NSIRA's annual public reports will be managed.

Clause 46 of the bill amends section 53 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*[17] to add new section 53.4, which indicates that disclosures of information to the NSIRA from the Financial Transactions and Reports Analysis Centre (FINTRAC) will be made through the Minister of Finance, rather than directly by the director of FINTRAC. This provision essentially shields FINTRAC from direct contact with the NSIRA.

2.1.3 Annual Reports

Under section 38(1) of the NSIRA Act, the prime minister is to receive an annual report addressing NSIRA activities, findings and recommendations for the previous calendar year, a copy of which is required to be tabled in both the Senate and the House of Commons within 15 sitting days of the report's being submitted to the prime minister.

Section 39 of the NSIRA Act requires the NSIRA to provide a report on disclosures made under the amended *Security of Canada Information Sharing Act*, renamed *Security of Canada Information Disclosure Act* under Bill C-59,[18] to the Minister of Public Safety and Emergency Preparedness.

Under section 40, where the NSIRA has undertaken a special report that it believes is in the public interest, the report is to be submitted to the appropriate minister.

In both cases, the minister is required to table a copy of the report in the Senate and the House of Commons within 15 sitting days of receiving it.

Some current SIRC reporting requirements will not be continued by the NSIRA. For example, the current regime requires SIRC's annual report to include the number of warrants issued in the fiscal year under section 21.1 of the *Canadian Security Intelligence Service Act* (CSIS Act),[19] as well as the number of applications for warrants made under that section that were refused in that year. No such reporting requirement is set out in Bill C-59.

2.1.4 Secretariat

Section 41 of the NSIRA Act establishes the NSIRA Secretariat to assist the Agency in fulfilling its mandate.

As set out in section 42 of the NSIRA Act, the executive director of the NSIRA Secretariat is appointed by the Governor in Council for a term of up to five years, and the term may be renewed. Sections 45 and 46 describe the broad authority of the executive director, who, under section 42, has the rank of a deputy head of a department, regarding the employment and termination of staff. That authority matches that of the Chief of CSE, as set out in section 13 of the Communications Security Establishment Act (CSE Act, found in clause 76 of Bill C-59).

Under clause 30 of Bill C-59, the NSIRA Secretariat is listed as a separate agency under Schedule V of the *Financial Administration Act*,[20] meaning that it is part of the public service and subject to the *Public Service Employment Act* (PSEA).[21] Under section 35(1) of the PSEA, unless explicitly prohibited, employees of separate agencies have mobility to and from other parts of the public service. This means, for example, that employees of national security and intelligence agencies could work for the NSIRA Secretariat on secondment, and return to their home agencies afterward.

2.2 PART 1.1: AVOIDING COMPLICITY IN MISTREATMENT BY FOREIGN ENTITIES ACT (CLAUSES 49.1 AND 49.2)

Part 1.1 of Bill C-59 enacts An Act respecting the disclosure of and request for information that would result in a substantial risk of mistreatment of an individual by a foreign entity and the use of information that is likely to have been obtained as the result of mistreatment of an individual by a foreign entity (short title: Avoiding Complicity in Mistreatment by Foreign Entities Act [ACMFEA]). Under section 3 of the Act, the Governor in Council is empowered to issue directions concerning disclosure of, requests for, and use of information that would result in a high risk of mistreatment of a person. The ACMFEA directs the Governor in Council to issue such directions to these deputy heads: the Chief of the Defence Staff, the Deputy Minister of National Defence, the Deputy Minister of Foreign Affairs, the Commissioner of the RCMP, the Director of CSIS, the President of the Canada Border Services Agency (CBSA), and the Chief of CSE. Sections 5 and 6, respectively, state that as soon as is feasible after receiving these directions, the deputy heads must make them public, and they must provide a copy to the National Security and Intelligence Committee of Parliamentarians (NSICOP), and if applicable, to the relevant review body.

Section 3(3) of the ACMFEA notes that directions issued under the Act are not statutory instruments.

Section 7 of the ACMFEA requires each deputy head who receives such directions to provide a report before 1 March of each year to the appropriate minister on the implementation of the directions, and, as soon as feasible, to also make a redacted version available to the public. Section 8 requires the minister to give copies to the NSICOP, to the NSIRA and, if applicable, to the Civilian Review and Complaints Commission for the RCMP.

2.3 PART 2: ENACTMENT OF THE INTELLIGENCE COMMISSIONER ACT (CLAUSES 50 TO 75)

Clause 50 of the bill enacts An Act respecting the office of the Intelligence Commissioner (short title: Intelligence Commissioner Act [ICA]), which creates an office of the Intelligence Commissioner. The Commissioner's duties and functions, as set out in section 12 of the ICA, are to provide oversight of a subset of CSE and CSIS activities. The Office of the Intelligence Commissioner replaces the Office of the CSE Commissioner.

Section 4 of the ICA stipulates that the Intelligence Commissioner must be a retired judge of a superior court.[22] Sections 4(1) and 4(2) of the ICA indicate that the Intelligence Commissioner will serve a five-year term, subject to good behaviour and renewable for an additional term of not more than five years.

The Department of Justice's Charter Statement says that the ICA will:

> establish an independent, quasi-judicial Intelligence Commissioner, who would assess and review certain Ministerial decisions regarding intelligence gathering and cyber security activities. This would ensure an independent consideration of the important privacy and other interests implicated by these activities in a manner that is appropriately adapted to the sensitive national security context.[23]

The bill does not specify the forum or standard of review that would be applicable to such decisions.[24]

Section 6(3) of the ICA states that for the purposes of Part 7 of the PSEA, which addresses political activities of employees, the Intelligence Commissioner is considered a deputy head, meaning that he or she is barred from engaging in any political activity other than voting in an election.

Like the executive director of the NSIRA Secretariat, the Intelligence Commissioner has considerable discretion regarding the employment and termination of staff. The language used in section 6(3) of the ICA to describe the powers of the Intelligence Commissioner in this regard reflects, almost word for word, language used to describe the powers of the Chief of CSE in section 13 of the CSE Act (found in clause 76 of Bill C-59).

Also as in the case of the NSIRA Secretariat, clause 65 of Bill C-59 adds the Office of the Intelligence Commissioner to the list of separate agencies in Schedule V of the *Financial Administration Act*, so that it is part of the public service and subject to the PSEA. This means, among other things, that under section 35(1) of the PSEA, employees of national security and intelligence agencies could work for the Office of the Intelligence Commissioner on secondment.

Clauses 51 to 59 of Bill C-59 provide for the transfer of Office of the CSE Commissioner resources to the Office of the Intelligence Commissioner.

2.3.1 Intelligence Commissioner Reviews

2.3.1.1 Powers

Section 12 of the ICA states that the Intelligence Commissioner is responsible for:

> (a) reviewing the conclusions on the basis of which certain authorizations are issued or amended, and certain determinations are made, under the *Communications Security Establishment Act* and the *Canadian Security Intelligence Service Act*; and
>
> (b) if those conclusions are reasonable, approving those authorizations, amendments and determinations.

As described in sections 13 and 14 of the ICA, the "certain authorizations" referenced in section 12 of the ICA are issued primarily by the minister responsible for CSE (currently, the Minister of National Defence)[25] on written application by the Chief of CSE, and they pertain to CSE foreign intelligence collection and cybersecurity activities.[26] Specifically, in instances where CSE proposes to undertake foreign intelligence collection or cybersecurity activities that may contravene an Act of Parliament, it must seek a ministerial authorization, and the Intelligence Commissioner must approve this authorization.[27] Under sections 15 and 18 of the ICA, respectively, the Commissioner must also review the reasonableness of amendments to such authorizations and the conclusions underlying any authorizations by the Director of CSIS permitting a query of datasets under exigent circumstances. As defined in clause 110 of Bill C-59, in the amended CSIS Act, a "dataset" is "a collection of information stored as an electronic record and characterized by a common subject matter."

The term "determinations" in section 12 references decisions made by the Minister of Public Safety and Emergency Preparedness to authorize CSIS to collect Canadian datasets or retain foreign datasets, as set out in sections 16 and 17 of the ICA. The minister will also make determinations about the justification in law for CSIS to commit classes of acts or omissions that would otherwise constitute offences. Specifically, the minister's determinations will provide the basis for designated CSIS employees to commit, or direct another person to commit, otherwise unlawful acts or omissions in furtherance of CSIS's information and intelligence collection and its threat reduction mandates (section 19 of the ICA, and new section 20.1 of the CSIS Act, set out in clause 101 of the bill).

Under sections 23(1) and 26 of the ICA, the Intelligence Commissioner will have right of access to all information, other than Cabinet confidences, that was before the person making the decision the Commissioner is reviewing, including information subject to solicitor–client privilege. Section 25 states that the ministers responsible for CSIS and CSE, as well as CSIS and CSE directly, may disclose additional information to the Commissioner. Further, clause 75 of the bill, which amends section 24 of the ICA, entitles the Intelligence Commissioner to receive reports from the NSICOP and the NSIRA.

2.3.1.2 Decisions

Section 20 of the ICA requires all Intelligence Commissioner decisions to be provided in writing. With respect to new and amended authorizations for CSE foreign intelligence collection and cybersecurity activities, determinations by the Director of CSIS related to Canadian datasets, and authorizations by the Director of CSIS for queries of datasets under exigent circumstances, the Commissioner has two options: to approve the authorization or determination in question, or not to approve it. When reviewing the conclusions that formed the basis for decisions to retain foreign datasets, the Intelligence Commissioner has three options: to approve the authorization, to approve the authorization with conditions, or to refuse to approve the authorization. Reasons are required for all decisions.

Most of the Intelligence Commissioner's decisions must be made within 30 days of the Commissioner's receiving notice of the authorization, but under section 20(3)(b) of the ICA, CSE and CSIS may attempt to negotiate a shorter time frame. Where the Director of CSIS has issued an authorization to query a Canadian or foreign dataset under exigent circumstances, the Commissioner is required to provide a decision as soon as feasible (section 20(3)(a) of the ICA and new section 11.22 of the CSIS Act, added under clause 97 of the bill). In clause 94 of the bill, a query is defined under the amended CSIS Act as "a specific search, with respect to a person or entity, of one or more datasets, for the purpose of obtaining intelligence."

Section 22 directs the Intelligence Commissioner to provide a report each calendar year to the prime minister on the Commissioner's activities. The report is to include statistics on the Commissioner's decisions to approve, amend or reject authorizations and determinations. It is up to the Commissioner to decide what statistics are appropriate to include in this annual report.

Prior to the Intelligence Commissioner's report being submitted to the prime minister, the Director of CSIS and the Chief of CSE are to vet it to remove any information that is subject to solicitor–client privilege, professional secrecy of advocates and notaries or to litigation privilege or information that would be injurious to national security, national defence or international relations. Once the prime minister has received the report, the prime minister must table a copy of it in both houses of Parliament within the first 15 days that each house is sitting.

2.3.1.3 Publicly Available Information and Datasets

CSE and CSIS collection of publicly available information is not subject to either ministerial authorization/determination or Intelligence Commissioner approval. To fulfill its duties and functions under sections 12 to 16 of the CSIS Act, CSIS is permitted, in new section 11.11(1) of the CSIS Act, created under clause 97 of the bill, to retain, query and exploit publicly available datasets without a ministerial determination or the approval of the Intelligence Commissioner. Likewise, under section 23(1) of the CSE Act, CSE is permitted to acquire, use, analyze, retain and disclose publicly available information in the furtherance of its mandate without ministerial authorization or the approval of the Intelligence Commissioner. Use of the term "disclosing" in the new authorities for CSE suggests that external entities will rely on publicly available information acquired and analyzed by CSE and that the intent is to routinize such disclosure.

"Publicly available information" is defined under section 2 of Bill C-59's new CSE Act as:

> information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise or is available to the public on request, by subscription or by purchase.

It appears that this definition would accommodate bulk acquisition of *any* publicly available information that has been published or broadcast for public consumption, including, for example, facial imagery captured in social media posts.[28] This suggests that CSE and CSIS may acquire publicly available information in bulk, meaning that the data would not be filtered to remove all non-target–related information. Further, both agencies would be empowered to analyze or exploit the publicly available information they acquire, activities which suggest knowledge discovery through data mining. Given that the definition of "publicly available" also accommodates payment for access to information, service providers and information brokers may be incentivized to collect and sell to CSE new forms of information packages on users. Among the information broker products that are already available to those willing to pay are credit histories, web browsing history, online purchases, social-media connections, marital status, and a variety of information that enables the construction of detailed personal profiles.

While CSE bulk collection of publicly available datasets may not be subject to Intelligence Commissioner oversight, there are other CSE and CSIS activities that entail collection and retention of massive datasets over which the Intelligence Commissioner will have jurisdiction. These activities involve collection of information that is not publicly available (new section 26(2)(b) of the CSE Act and new sections 11.01 to 11.25 of the CSIS Act).

In the case of CSE foreign intelligence collection, data is sometimes be collected in bulk, meaning that CSE acquires information for technical and operational purposes without the use of specific, foreign intelligence target–related filters, such as telephone numbers and email addresses. Given the unpredictable way that communications are routed through the global information infrastructure[29] and the lack of filtering used in the collection process, Canadian metadata, such as Internet protocol addresses, may be incidentally collected as part of these bulk foreign datasets. Information acquired in this manner is referred to in Bill C-59 as "unselected," defined in section 2 of the CSE Act as information that is "acquired, for technical or operational reasons, without the use of terms or criteria to identify information of foreign intelligence interest."[30] Under section 34(2) of the CSE Act, to approve a ministerial authorization to collect foreign intelligence in bulk, the Intelligence Commissioner will need to judge as reasonable the minister's conclusion that no other reasonable means exists to acquire the information and that information pertaining to Canadians or persons in Canada will only be used, analyzed or retained if it is essential to international affairs, defence or security.

For its part, and subject to the Intelligence Commissioner's approval, CSIS can collect approved classes of Canadian datasets and is permitted to retain certain foreign datasets. References in amendments to "classes" of datasets whose evaluation and characterization may require up to 90 days, contained in new section 11.07(1) of the CSIS Act as provided in clause 97 of the bill, may indicate that CSIS will leverage "big data" analysis to fulfill its security intelligence mandate.

2.4 PART 3: ENACTMENT OF THE COMMUNICATIONS SECURITY ESTABLISHMENT ACT (CLAUSE 76)

2.4.1 The Communications Security Establishment

Clause 76 of the bill removes CSE's mandate from the *National Defence Act* (NDA) and creates a separate enabling statute, An Act to establish the Communications Security Establishment (short title: Communications Security Establishment Act [CSE Act]). In the main, the CSE Act empowers CSE to collect publicly available information in bulk, including information on Canadians, to collect foreign intelligence, and to conduct cyber-enabled threat reduction operations against foreign entities using covert means.

The new Act appears to shift the focus of CSE's enabling authorities. The NDA sets out strict conditions for the CSE to violate Part VI of the *Criminal Code*,[31] which prohibits interception of private communications, while the CSE Act provides the basis for CSE both to intercept private communications and to commit a much broader range of offences, most of which are unspecified (sections 3 and 49 to 51 of the CSE Act).

Section 2 of the CSE Act proposes a definition for federal institutions covered by CSE's mandate that includes Parliament and its institutions, federal courts, and government departments and agencies. This means that CSE could provide cybersecurity advice and services for organizations in all three branches of government. The breadth of this definition could have implications with respect to constitutional separation of powers. Both the federal courts and the Supreme Court of Canada have threatened to mount a constitutional challenge in the face of government efforts to force them to use the information technology services provided by Shared Services Canada, which include CSE cybersecurity monitoring, on the grounds that to do so would threaten their independence.[32]

Under section 4 of the CSE Act, the Governor in Council may, by order, designate any federal minister to be responsible for CSE. This suggests that the Minister of National Defence may not remain the minister responsible for the CSE.

2.4.1.1 Mandate

The CSE Act expands CSE's current mandate from three to five parts. Whereas CSE is currently mandated to acquire foreign intelligence from the global information infrastructure, help protect government electronic information and networks, and provide technical and operational support to federal law enforcement and national security agencies; section 15(2) of the CSE Act adds defensive and active cyber operations to the CSE's mandate.

Section 47 of the CSE Act – by directing that the minister must personally exercise the powers set out in sections 26(1), 27(1) and 27(2), 29(1), 30(1), 36(2), 39(1) and 40(1) – ensures that the minister cannot delegate the authorization or amended authorization of any of CSE's five mandated activities.

Of note is the expansion of CSE's foreign intelligence mandate under section 16 to include acquisition by covert means. Though CSE currently makes efforts to hide its foreign intelligence collection activities from its targets, explicitly authorizing it to use covert means opens up a larger range of operational possibilities. New section 26(2)(d) of the Act states that the minister can authorize CSE to "do anything that is reasonably necessary to maintain the covert nature" of a foreign intelligence collection activity.[33]

CSE's active cyber operations may also make use of covert means. Though the word "covert" does not appear in section 19 of the Act, which describes active cyber operations as activities intended 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 international affairs, defence or security," it does appear in section 31(c) under "Cyber Operations Authorizations." This section indicates that CSE may do "anything that is reasonably necessary to maintain the covert nature" of its active cyber operations.

Empowering CSE to undertake threat reduction activities against foreign targets independently of CSIS not only broadens the government's scope to address different types of concerns – for example, countering foreign social media–enabled influence operations and active measures – it also provides for CSE to undertake such operations in cooperation with foreign allied agencies.

Section 22 of the Act stipulates that none of CSE's activities – with the exception under section 23(1) for CSE collection of publicly available information – may be directed at Canadians or persons in Canada, infringe on the *Canadian Charter of Rights and Freedoms*,[34] or take place without ministerial authorization. It should be noted that an exception is also made in section 46 of the CSE Act for CSE to direct its activities at Canadians or persons in Canada to prevent imminent death or serious bodily harm.

2.4.1.2 Arrangements

With respect to collaboration with others, CSE is given explicit authorization under section 54 of the CSE Act to enter into arrangements with foreign and domestic entities that have similar powers and duties.

The term "entity" is defined in section 2 of the CSE Act as "a person, group, trust, partnership or fund or an unincorporated association or organization and includes a state or a political subdivision or agency of a state." Thus, along with foreign signals intelligence, human intelligence or cybersecurity agencies, international organizations, and the institutions of international organizations, this definition includes domestic institutions and organizations. The Canadian Cyber Threat Exchange, or CCTX, is one domestic entity with which CSE has already established a relationship.[35] CSE's new Canadian Centre for Cyber Security, created under the *Budget Implementation Act, 2018, No. 1* and operational as of 1 October 2018, will likely pursue cooperative arrangements with public and private sector partners.

To further CSE's mandated activities, section 54 empowers the Establishment to enter into arrangements with entities not only for the purposes of information sharing but also of "otherwise cooperating with them." This language may open the door to CSE's undertaking active and defensive cyber operations, using covert means, in cooperation with foreign signals intelligence agencies. None of these operations would be subject to Intelligence Commissioner review and approval. However, under sections 29 and 30, prior to entering into an arrangement with a foreign institution or organization, CSE must obtain the minister's approval, which can be provided only after the minister has consulted with the Minister of Foreign Affairs.

2.4.1.3 Defensive and Active Cyber Operations

Section 18 of the CSE Act describes defensive cyber operations as activities carried out "on or through the global information infrastructure to help protect" electronic information and information infrastructures. However, language in section 29(1) of the CSE Act indicating that the minister may authorize a defensive cyber operation "despite any other Act of Parliament or of any foreign state" suggests that defensive cyber operations might not be entirely passive. Such operations could contravene domestic laws and, unless conducted with the consent of a host state, they would almost certainly contravene foreign laws.

As set out in sections 29(2) and 30(2) of the CSE Act, the minister may only authorize defensive and active cyber operations, respectively, after having consulted with or obtained the consent of the Minister of Foreign Affairs. This requirement suggests that such operations entail risk to Canada's international affairs.

The Department of Justice's Charter Statement on section 34 (formerly section 33) would seem to support the view that foreigners and their property will not be subject to the same degree of operational restraint as Canadians and their property.[36]

Though no prior approval of the Intelligence Commissioner is required under the CSE Act for either defensive or active cyber operations, the NSIRA will be empowered under section 8(1)(a) of the NSIRA Act to conduct *ex post* (after the fact) reviews of the lawfulness, reasonableness and necessity of such operations.

Sections 27(1) and 27(2) of the CSE Act respectively establish that CSE is authorized to conduct cybersecurity operations to help protect federal and non-federal institutions and infrastructures designated by the minister under section 21(1) as being "of importance to the Government of Canada." In other words, CSE can take a more direct hand in protecting private-sector–owned and –operated critical information infrastructures, an authority that it already has under section 273.64(1)(b) of the NDA but which, to date, it has not exercised in any systematic way.

Section 32 prohibits CSE from engaging in certain conduct as part of its defensive and active cyber operations. CSE is barred from causing bodily harm[37] to an individual and from obstructing, defeating or perverting the course of justice or democracy. This mirrors language found in section 12.2 of the CSIS Act, outlining threat reduction provisions, with one significant exception: unlike CSIS, CSE is not explicitly prohibited from violating the sexual integrity of an individual.

2.4.1.4 Ministerial Authorizations

Section 33 of the CSE Act describes the procedures to be used in applying for a ministerial authorization and the conditions that must be met for the minister to give authorization.

When CSE seeks ministerial authorization to engage in cybersecurity activities involving non-federal infrastructures, section 33(3) requires it to include a written request for cybersecurity assistance from the infrastructure owner in its authorization request. CSE does not require a written request for cybersecurity assistance from government departments, parliamentary institutions or federal courts prior to rendering such assistance. However, as part of the conditions CSE must satisfy before the minister can conclude that there are reasonable grounds to believe that it is reasonable and proportionate to issue a cybersecurity authorization for federal institutions, under section 34(3)(b) of the CSE Act, CSE must demonstrate that it could not reasonably obtain the consent of all persons whose information may be acquired in the course of its activities.

Section 35 of the CSE Act describes the contents of ministerial authorizations sought to conduct foreign intelligence collection (section 26(1)), cybersecurity assistance to federal or non-federal institutions (sections 27(1) and 27(2)), defensive cyber operations (section 29(1)), or active cyber operations (section 30(1)). Among other things, these contents spell out the "what, who and when" of the authorization, describing, for example, the activities or classes of activities CSE is authorized to conduct; the persons or classes of persons who are authorized to conduct these activities or classes of activities; and the dates for authorization to come into effect and expire. The ministerial authorizations must also articulate any terms, conditions or restrictions the minister has placed on his or her authorization, including privacy protection measures and measures to ensure the reasonableness and proportionality of the activities. For example, section 35(f) of the Act requires CSE to indicate whether a foreign intelligence collection activity will include bulk collection and "any terms, conditions or restrictions the minister considers advisable to limit the use, analysis and retention of, and access to," this "unselected information."

Section 36(2) empowers the minister to extend the period of validity for a foreign intelligence or cybersecurity authorization by up to a year. Though, under section 36(3), the minister's decision is not subject to Intelligence Commissioner review, section 36(4) requires the minister to notify the Commissioner of any such extension as soon as is feasible.

Section 37(1) of the CSE Act directs the chief of CSE to notify the minister of any significant change to a fact used to obtain a ministerial authorization as soon as possible. Section 37(2) grants the minister discretion in reporting the changed factual basis to the Intelligence Commissioner, directing the minister to report such changes only if the authorization is subject to Intelligence Commissioner approval and the minister concludes that the change is significant.

Section 37(3) of the CSE Act stipulates that if the minister concludes that the factual basis underlying an authorization for active or defensive cyber operations not subject to Intelligence Commissioner approval has changed significantly, the minister must inform the NSIRA of his or her conclusions.

If the minister concludes that there is a significant change in the facts underlying an authorization, section 39 provides the possibility of issuing an amended authorization for the Intelligence Commissioner's review and approval. Of note is that under section 39(3), a foreign intelligence or cybersecurity activity being conducted under an authorization that must be amended because of significant factual changes continues to be authorized until an Intelligence Commissioner–approved amended authorization comes into force.

2.4.1.5 Emergency Foreign Intelligence or Cybersecurity Authorization

Section 40 of the CSE Act empowers the minister to issue an emergency foreign intelligence or cybersecurity authorization if he or she concludes that there are reasonable grounds to believe that the conditions to authorize such activities have been met but that the time required to obtain the Intelligence Commissioner's approval would defeat the purpose of issuing an authorization under normal procedures. Section 40(2) states that the Intelligence Commissioner is not entitled to review an emergency authorization. However, under section 41, the Intelligence Commissioner and NSIRA must both be notified of all emergency authorizations as soon as feasible, and, as set out in section 42, the emergency authorization is valid for only five days.

Procedurally, an application to the minister for an emergency authorization differs from that made under normal circumstances in one respect: section 40(3) of the CSE Act states that it can be delivered orally and must provide the minister with reasonable grounds to believe that the time required to obtain Intelligence Commissioner approval would defeat the purpose of issuing an authorization under normal procedures.

Even if an application for an emergency cybersecurity authorization to access and acquire information from a non-federal infrastructure is made orally, section 40(4) of the Act requires that the owner or operator of the non-federal information infrastructure provide the minister with a written request for such assistance.

2.4.1.6 Protection of Privacy

Section 24 of the CSE Act requires CSE to undertake measures to protect the privacy of Canadians and persons in Canada regarding the use, retention, analysis and disclosure of information *acquired* as part of the CSE's foreign intelligence collection, cybersecurity activities or collection of publicly available information. This language is notable because it expands CSE's existing privacy protection regime to include non-citizens present in Canada.

The word "acquired" is highlighted above to further emphasize an important distinction between the current and new CSE mandates. Use of the word "acquired" in the new mandate may be a response to concerns that the CSE Commissioner and the privacy commissioner have raised about ambiguous language in the NDA, as well as about how CSE collects and shares metadata.[38]

The term "acquire" is used in CSE's current mandate in connection with its foreign intelligence collection activities. Specifically, section 273.64(1)(a) of the NDA mandates CSE to "*acquire* and use information from the global information infrastructure for the purpose of providing foreign intelligence" [Authors' emphasis]. However, another term is used to specify the type of information to which CSE must apply privacy protection measures. Section 273.64(2) of the NDA requires CSE to undertake measures to protect the privacy of Canadians in the use and retention of *intercepted* information. Though neither "acquire" nor "intercept" are defined in the existing CSE mandate, interception of a private communication is defined in section 183 of the *Criminal Code* as including to "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof."

The term "acquire" as used in the *Criminal Code* definition refers to the act of obtaining a communication, but it also denotes the act of recognizing the communication's meaning or significance, thus implying a step that occurs subsequent to the collection of information. At one time, it went without saying that the act of recognizing the meaning or significance of a communication was undertaken by a human but, with the advent of artificial intelligence, this may not necessarily be the case. Officials with the United Kingdom's Government Communications Headquarters (CSE's counterpart) have been cited in the British media highlighting human interaction as the point where privacy concerns are raised, saying:

> The interception of a communication as it flows through a fibre optic cable does not entail a substantial invasion of privacy … unless that communication is selected for examination: in other words, unless a human examines it or may potentially examine it.[39]

Similarly, the British Security Service (CSIS's counterpart), uses the same logic, telling the Investigatory Powers Tribunal that:

> It is also relevant to note that as BPD's [bulk personal datasets] are searched electronically there was inevitably significantly less intrusion into individuals' privacy, as any data which has not produced a "hit" will not be viewed by the human operator of the system, but only searched electronically.[40]

Based on the wording of sections 273.64(1)(a) and 273.64(2) of the NDA, CSE also currently appears to make a distinction between the acquisition of information and the interception of it. Essentially, the information CSE acquires under its foreign intelligence and cybersecurity mandates is only considered

intercepted when a human (often assisted by a machine) has interacted with it in some way to recognize its substance, meaning or purport. This understanding would accord with CSE's long-standing argument that, prior to interception, it cannot predict if the information it will acquire under its foreign intelligence mandate contains private communications. Thus, under CSE's existing mandate, information acquired through automated means and maintained in a data buffer is not considered intercepted until an analyst has queried it using a search tool.

2.4.1.7 Disclosure of Information

Section 43 of the CSE Act provides that CSE may disclose to persons or classes of persons designated by the minister under section 45 any information that could be used to identify a Canadian or a person in Canada – essentially, metadata – collected under the Act's section 26(1) foreign intelligence mandate. In determining whether it should disclose such information and communications, CSE must conclude that "the disclosure is essential to international affairs, defence, security or cybersecurity." This essentiality test appears to consolidate existing elements of the essentiality tests set out in sections 273.65(2)(d) and 273.65(4)(d) of the NDA that CSE currently applies to disclosures made under its foreign intelligence and cybersecurity mandates.

To help protect federal and designated electronic information and infrastructures, section 44 of the CSE Act provides for disclosure of both metadata and intercepted private communications (content). This provision reflects the fact that malicious code used in cyber attacks is often embedded in the content of emails or in email attachments, both of which constitute private communications.

Section 46(1) of the Act empowers CSE to use or analyze information relating to a Canadian or a person in Canada if it has reasonable grounds to believe that there is an imminent danger of death or serious bodily harm to any individual and that the information would be relevant to the imminent danger. Section 46(2) authorizes CSE to disclose this information "to any appropriate person" if disclosure may help prevent death or serious bodily harm.

The Department of Justice's Charter Statement on section 46 (formerly section 47) of the CSE Act provides additional information. It notes that the information which provides CSE reasonable grounds to believe that there is an imminent danger of death or serious bodily harm "may have been incidentally discovered by CSE in the course of authorized activities, or may be provided by another agency or individual."[41] If CSE has collected information about a Canadian incidentally, it is likely a result of its foreign intelligence collection activities. Otherwise, the Charter Statement indicates that the information providing CSE with reasonable grounds to believe that there is an imminent danger could come from another agency or individual. The latter two sources should prompt questions about the credibility of the other agency's or the individual's information. Was the information the product of torture, for example, or could it be corroborated using other sources?

It is important to bear in mind that the disclosure of information under section 46 will likely result in law enforcement or, possibly, military actions. Use of the phrase "reasonable grounds to believe" in this provision is a recognized standard in criminal law and signals that CSE must have a high degree of certainty about the danger and the relevance of the information to the danger. However, it is equally noteworthy that the threshold for the CSE to disclose information – disclosure "may" prevent death or serious bodily harm – is much lower.

The Charter Statement goes on to say that "[t]he use and disclosure of potentially private information in these circumstances *may* engage section 8 of the Charter" [authors' emphasis]. Section 8 of the Charter states that "[e]veryone has the right to be secure against unreasonable search and seizure." The Department of Justice's use of the word "may" in respect of section 8 allows for a case-by-case assessment of the character of the information to be disclosed (e.g., is it the content of a communication or is it metadata?) and an assessment of whether CSE's proposed use and disclosure of it constitute search and seizure. Also to be considered is whether and how the Charter applies to extraterritorial activities.

Based on the wording used in section 46 of the CSE Act and in the Charter Statement, it would appear that section 46 will permit CSE, under urgent circumstances, to bypass normal identity disclosure processes and immediately disclose the private communications or Canadian-related metadata to individuals, including individuals working for foreign states or entities and corporations. The Department of Justice's statement that the objective of preventing imminent death or serious bodily harm "may serve to justify the use of information already in CSE's possession" appears to suggest that CSE may also be justified in the circumstances to query its bulk collection holdings for additional information that could be relevant to the imminent danger.

Section 46(3) of the CSE Act directs the chief of CSE to notify the minister in writing as soon as feasible if CSE has used, analyzed or disclosed information under section 46 provisions. The minister is then required to notify the NSIRA, although no time frame is attached to this requirement.

Section 55 of the Act prohibits the forced disclosure in court proceedings of the identity of any person or entity that has assisted or is assisting the CSE on a confidential basis. This prohibition against compelled disclosure includes any information from which the identity of the person or entity could be inferred. A designated Federal Court judge could authorize disclosure only if:

- the person or entity did not assist the CSE;
- the identity of individuals or entities could not be inferred from the information to be disclosed; or
- the information is necessary to establish the accused's innocence in the prosecution of an offence.

2.4.1.8 Regulations

In addition to conferring general regulation-making powers, section 60(c) of the CSE Act empowers the executive branch to change through regulations "the definition of any term defined in section 2 or section 23(5) or 44(3) to respond, directly or indirectly, to any technological change." This provision essentially permits the government to amend the CSE Act through subordinate legislation, which engages a much lower level of parliamentary scrutiny than does legislation, and scrutiny that would occur only after the regulation has come into force.[42]

2.4.1.9 Civil and Criminal Liability

Sections 49 through 51 of the CSE Act provide shields against liability for a broad range of CSE activities. Section 49 shields from criminal and civil liability persons acting in accordance with a ministerial authorization or persons who, in good faith, assist a person they have reasonable grounds to believe is acting in accordance with a ministerial authorization. Thus, if a CSE employee or a person assisting CSE's authorized cybersecurity activities causes damage to a telecommunications provider's infrastructure, the provider may not be able to claim for damages.

Section 50 protects CSE from liability under Part VI of the *Criminal Code* in relation to the CSE's interception and subsequent use, analysis, retention and disclosure of private communications obtained under ministerial authorization. Section 51 shields the Crown from liability under section 18 of the *Crown Liability and Proceedings Act*,[43] which pertains to using or disclosing an intercepted private communication. Both sections 50 and 51 differ little from existing provisions in sections 273.69 and 273.7 of the NDA.

2.4.1.10 Reporting Requirements

Section 52 of the CSE Act contains reporting requirements that direct the chief of CSE to report on the outcome of activities carried out under ministerial authorizations within 90 days of the last day of validity. The minister, in turn, must provide a copy to the Intelligence Commissioner and the NSIRA.

Under section 59 of the CSE Act, within three months after the end of the fiscal year, CSE must publish an annual report on its activities for that year.

2.5 PART 4: AMENDMENTS TO THE *CANADIAN SECURITY INTELLIGENCE SERVICE ACT* (CLAUSES 92 TO 111)

2.5.1 Datasets

2.5.1.1 Background

Part 4 of the bill amends the *Canadian Security Intelligence Service Act* (CSIS Act) in large part to create regimes for judicial authorizations and Intelligence Commissioner–approved authorizations for CSIS dataset collection and retention. One regime is used for Canadian datasets, while another applies to foreign datasets.

As defined in amended section 2 of the CSIS Act, "dataset" means "a collection of information stored as an electronic record and characterized by a common subject matter." A "Canadian dataset" is a dataset that relates mainly to individuals within Canada or Canadians. A "foreign dataset" is a dataset that relates mainly to individuals who are not Canadian and who are outside Canada or corporations that are not incorporated in Canada and who are outside Canada.

In part, the amendments to the CSIS Act can be viewed as a response to the court case called *X (Re)*, in which Federal Court Justice Simon Noël found that CSIS had failed in its duty of candour by not informing the Court that for the previous decade it had been retaining non-target–related data collected under warrant.[44] The decision was based on the fact that CSIS was storing this "associated data" – essentially, third-party communications metadata, but not content – in its Operational Data Analysis Centre (ODAC). ODAC personnel were using computational tools to analyze this metadata along with data stored in other CSIS holdings, and providing any resulting insights to CSIS investigators to assist in their work.

Justice Noël held that the CSIS Act authorizes CSIS to collect and retain only that information which "is strictly necessary" to carry out its mandate. He further ruled that warrants issued under section 21 of the CSIS Act only authorize CSIS to collect information on threats to the security of Canada, as defined by section 2, and in the context of the authorities set out in sections 12 through 16. CSIS's retention of associated data, he said, falls outside of its legislatively defined jurisdiction and does not respect its limited primary mandate and functions.[45]

2.5.1.2 Dataset Collection, Retention and Creation

Under new section 11.05 of the CSIS Act, provided for in clause 97 of Bill C-59, CSIS is authorized to collect datasets if it reasonably believes these datasets are publicly available, belong to an approved class, or predominantly relate to non-Canadians who are outside of Canada.

Clause 102 of Bill C-59 amends section 21 of the CSIS Act to permit CSIS to apply for judicial authorization to retain information that is collected incidentally under a warrant issued for the purpose of section 12 and to create datasets from it. Section 12 empowers CSIS to collect, analyze and retain information on activities believed to constitute threats to Canadian security.

To authorize retention of incidentally collected information, the judge to whom the application is made must be satisfied that the information will assist CSIS in its activities under sections 12, 12.1 and 16 of its mandate, which pertain to CSIS's duties and functions:

- As mentioned above, section 12 provides that CSIS may collect, analyze and retain information and intelligence respecting threats to the security of Canada and report on these threats to the Government of Canada.
- Section 12.1 empowers CSIS to undertake measures to reduce security threats.
- Section 16 empowers CSIS to assist the Minister of National Defence and the Minister of Foreign Affairs by collecting foreign intelligence inside Canada.

2.5.1.3 Publicly Available Datasets

CSIS collection of publicly available datasets, which are defined under new sections 11.01 and 11.07 of the CSIS Act as information that was "publicly available at the time of collection," is subject to neither judicial nor Intelligence Commissioner supervision. However, limits are placed on CSIS collection of such datasets. New section 11.11(1) of the CSIS Act stipulates that CSIS may only retain, query and exploit a publicly available dataset for the purposes of sections 12 to 16, relating to CSIS' mandate. New section 11.11(2) of the CSIS Act imposes the same mandate-related strictures on CSIS retention of the results of any queries or exploitation of publicly available datasets. As defined in amended section 2 of the CSIS Act, exploitation is "a computational analysis of one or more datasets for the purpose of obtaining intelligence that would not otherwise be apparent." In other words, exploitation is data-mining using algorithms (which are essentially rule-sets) to discover patterns and connections.

New section 11.24(1)(a) of the CSIS Act directs CSIS to maintain records of its publicly available datasets. These records must provide the rationale for the collection of the datasets, detail each exploitation and the results of each exploitation and query, and articulate the statutory provision under which the results of each exploitation and query has been retained. CSIS is required under section 11.24(1)(b) to periodically and randomly verify that results obtained from queries and exploitation have been retained for the purposes of sections 12 to 16 of the CSIS Act. New section 11.25 specifies that the results of these verifications are to be shared with the NSIRA.

2.5.1.4 Dataset Evaluation, Retention and Destruction

New sections 11.24(2) and 11.24(3) direct CSIS to maintain and verify records for approved classes of Canadian and foreign datasets, with access limited to designated employees. As with publicly available datasets, the results of periodic and random verification that the information is being appropriately retained are to be shared with the NSIRA. In addition, new section 11.25 specifies that the NSIRA is to be informed of any removal of information from a foreign dataset that by its nature or attributes relates to a Canadian or a person in Canada.

One of the issues raised by Justice Noël in his decision in *X (Re)* (see section 2.5.1.1 of this Legislative Summary) was that CSIS was storing information, some of which it had no authority to retain, for indefinite periods. To respect its legal mandate, he stated, CSIS needs to assess data it has collected under warrant as soon as possible so that information it has no legal authority to retain can be destroyed promptly. The amendments Bill C-59 puts forward in new section 11.07(1) appear to respond to this concern.

As soon as feasible, but no later than 90 days after a dataset is collected, designated CSIS employees must evaluate the dataset to confirm whether it:

> (a) was publicly available at the time of collection;
>
> (b) predominantly relates to individuals in Canada or Canadians; or
>
> (c) predominantly relates to individuals who are not Canadians and who are outside Canada or corporations that were not incorporated or continued under the laws of Canada and who are outside Canada.

New section 11.07(6) of the CSIS Act requires that, during the period of dataset evaluation, the designated employee delete any personal information which, in the opinion of CSIS, is not relevant to the performance of the organization's duties and functions and may be deleted without affecting the integrity of the dataset.

In accordance with new section 11.1(1)(a) of the CSIS Act and regardless of whether the dataset is Canadian or foreign, the designated employee must delete any information where there is a reasonable expectation of privacy related to an individual's mental or physical health.[46] New section 11.1(1)(b) requires that, if the dataset is evaluated as Canadian, the designated employee delete any information that is subject to solicitor–client privilege or the professional secrecy of advocates. New section 11.1(1)(c) requires that, if the dataset is evaluated as foreign, the designated employee eliminate any information that by its nature or attributes relates to a Canadian or a person in Canada.

If a foreign dataset is evaluated as predominantly relating to individuals in Canada or Canadians, under new section 11.07(2), the designated employee must then determine whether it is part of an approved class of datasets. As described in new section 11.01 of the CSIS Act, an approved class of datasets is a Canadian dataset whose collection has been authorized by the Minister of Public Safety and Emergency Preparedness and approved by the Intelligence Commissioner. If the dataset is evaluated as not belonging to any approved class, CSIS must either destroy it immediately or ask the minister for the determination of a new class to which it would belong.

Under new section 11.03(2), in considering a request for a new class of Canadian approved dataset, the minister must determine that querying or exploiting the dataset will lead to "results that are relevant to the performance of the Service's duties and functions set out under sections 12, 12.1 and 16," pertaining to CSIS's security intelligence collection and analysis mandate, its threat reduction mandate, and its mandate to collect foreign intelligence within Canada. If the minister determines that collection of the dataset should be authorized, he or she must notify the Intelligence Commissioner so that the latter can review the minister's determination for reasonableness. It is not clear if the minister is required to notify the Intelligence Commissioner when a determination is made that dataset collection should not be authorized, but the wording of section 11.08(4) of the CSIS Act suggests this will not be required.

New section 11.07(3) of the CSIS Act specifies that during the period of evaluation and up until the Intelligence Commissioner approves the minister's determination, CSIS is not permitted to query or exploit the dataset. Only after the Intelligence Commissioner approves the determination in a written decision provided to the appropriate minister can an authorization be considered valid. If the Intelligence Commissioner does not find the conclusions leading to an authorization or amendment reasonable, he or she must withhold approval and provide reasons for having done so in writing to the minister.

If it wishes to retain a Canadian dataset, CSIS must seek judicial authorization under new section 11.13 of the CSIS Act. In issuing an authorization, the judge must be satisfied that retention of the dataset will assist CSIS in the performance of its duties and functions under sections 12, 12.1 and 16 of the Act and that CSIS has removed any information that relates to the physical or mental health of a person or any information that is protected under solicitor–client privilege or the professional secrecy of advocates and notaries. New section 11.14(2) specifies that such authorizations will be valid for no longer than two years.

Among other things, new section 11.13(2) of the CSIS Act requires that the application inform the judge whether the director of CSIS or a designated employee has identified any exceptional or novel privacy concerns. Under new section 11.14(1), in issuing an authorization, the judge must specify any terms and conditions placed on the exploitation or querying of the dataset, as well as its destruction. The judge must also specify any terms or conditions that he or she feels are in the public interest.

If the judge refuses to authorize the retention, subject to the time frame required to make or exhaust all rights of appeal, new section 11.15(1) of the CSIS Act requires CSIS to destroy the Canadian dataset without delay.

Under new section 11.17, the minister or a designated person may make a determination to authorize retention of a foreign dataset.[47] The period of authorization cannot exceed five years beyond the day the Intelligence Commissioner approves it. As specified in section 11.19(3), if CSIS has not made a new request for authorization to retain a foreign dataset before the expiration of the previous authorization, it must destroy the dataset within 30 days of that expiry date.

To authorize retention of the dataset, the minister or the designated employee must come to the following conclusions:

- that the dataset relates predominantly to foreign individuals or corporations;
- that the dataset is likely to assist CSIS in the performance of its duties and functions under sections 12, 12.1, 15 and 16 of the CSIS Act; and
- that CSIS has deleted any information in the dataset where there is a reasonable expectation of privacy concerning an individual's physical or mental health and any information that by its nature or attributes relates to a Canadian or a person in Canada.

2.5.1.5 Exigent Circumstances

New section 11.22(1) empowers the director of CSIS to authorize a designated employee to query a Canadian dataset that is not subject to a valid judicial authorization issued under new section 11.13 or a foreign dataset that is not subject to a valid authorization issued under new section 11.17 (meaning the Intelligence Commissioner has not approved the authorization) if the director concludes that:

- the dataset was collected under new section 11.05(1) of the CSIS Act, which requires CSIS to collect a dataset only if it is satisfied that the dataset is relevant to the performance of its duties under sections 12 to 16; and
- there are exigent circumstances that require a query of the dataset.

The director's new section 11.22 authorization is only valid after the Intelligence Commissioner has approved it in writing. As provided by new section 11.22(2), the authorization must provide a description of the exigent circumstances, a description of the dataset to be queried and the grounds on which the director concluded that the query will likely produce intelligence that would preserve the life or safety of an individual or intelligence of significant national security value that would be lost if CSIS followed normal procedures.

New section 11.22(2.1) stipulates that CSIS may only retain the results of a dataset query carried out under exigent circumstances if:

- the collection, analysis and retention of the results are carried out under section 12;
- the retention is strictly necessary to assist CSIS in the performance of its duties and functions under section 12.1; or
- the retention is required to provide section 16 assistance to the Minister of National Defence or the Minister of Foreign Affairs. Under section 16 of the CSIS Act, CSIS may assist the Minister of National Defence or the Minister of Foreign Affairs by collecting foreign intelligence within Canada.

2.5.1.6 Potential Unlawful Querying or Exploitation of Datasets

Under new section 27.1(1), found in clause 107 of the bill, if the NSIRA believes that any querying or exploitation of a dataset by CSIS under new sections 11.11 (publicly available dataset) and 11.2 (every dataset that contains personal information that does not directly and immediately relate to activities that represent a threat to the security of Canada) has not been lawful, it may provide the director of CSIS with the relevant sections of a report prepared under section 35 of the NSIRA Act and any other documentation it believes could help the Federal Court to make a determination under new section 27.1(4) of the CSIS Act. The NSIRA is directed in section 27.1(2) to ensure no information protected by solicitor–client, professional secrecy of solicitors and advocates, or litigation privilege is disclosed in the materials it provides to the director. New section 27.1(3) stipulates that as soon as feasible after receiving this information, the director must cause it and any other information the director believes may be relevant to be filed in the Federal Court.[48]

2.5.2 Threat Reduction Measures

Clause 98 of the bill amends section 12.1(2) of the CSIS Act to require the reasonably foreseeable effects on third parties, including those relating to privacy rights, to be taken into account when considering the use of threat reduction measures.

Section 12.1(3) of the CSIS Act is replaced by a number of provisions that, among other things, emphasize that the *Canadian Charter of Rights and Freedoms* is the supreme law in Canada and confirm that CSIS cannot undertake any measure that would limit a Charter right without authorization under a warrant. Further, a judge may issue such a warrant only if he or she is satisfied that the measures the warrant authorizes comply with the Charter.

New section 12.1(3.4) further underscores the lawfulness message by stipulating that CSIS cannot undertake any measure that might otherwise be contrary to a Canadian law without authorization under a warrant issued under section 21.1.

New section 12.1(3.5) introduces a requirement for CSIS to notify the NSIRA that it has undertaken threat reduction measures "as soon as the circumstances permit."

Clause 99 of the bill increases section 12.2(1) limitations imposed on CSIS threat reduction measures to include strictures against torture, detention and causing loss or serious damage to property that would endanger the safety of an individual.

Clause 103 of the bill amends section 21.1(1) of the CSIS Act, which pertains to applications for warrants to undertake measures to reduce threats to security in Canada. Among other things, the amendments specify that threat reduction measures include "altering, removing, replacing, destroying, degrading or providing – or interfering with the use or delivery of – any thing or part of a thing, including records, documents, goods, components and equipment" and impersonating a person other than a police officer to enable such actions.

Amended sections 21.1(2)(c), 22.1(1)(b) and 22.2 of the CSIS Act (contained in clauses 103 to 105 of the bill) each inject wording directing that the effects on third-party rights, including privacy rights, be taken into account in considering the reasonableness and proportionality of actions related to threat reduction measures.

2.5.3 Liability Shielding for Covert Activities

New section 18.2(1) of the CSIS Act, added by clause 100 of the bill, introduces various *Criminal Code* exemptions to protect CSIS employees and persons under CSIS direction from liability if, for the sole purpose of maintaining a covert identity:

- they make a false statement with respect to a covert identity;
- they make, request to be made, procure, use or transfer false documents; or
- they act on or authenticate a false document as if it were genuine.

Additional provisions appear to be intended to enhance accountability regarding the use of new CSIS information and intelligence collection authorities, particularly engagement in covert activities.

Among other things, clause 101 of the bill adds section 20.1 to the CSIS Act. This supplements the provisions in section 20, which pertains to the protection and conduct of CSIS employees, to require, under section 20.1(3), that the minister at least once a year issue an order determining:

> the classes of acts or omissions that would otherwise constitute offences and that designated employees may be justified in committing or directing another person to commit if the Minister concludes that the commission of those acts or omissions is reasonable.

In other words, the minister must make a list of the types of laws certain CSIS employees or persons under their direction are permitted to break in the course of their mandated work.

Under sections 20(2) and 20(3) of the CSIS Act, the director is required to submit a report to the minister and a copy to the attorney general if he or she is of the opinion that an employee has acted unlawfully in the performance of CSIS's duties and functions. However, there are occasions where such acts and omissions are reasonable in relation to the employee's role in carrying out CSIS's duties and functions. For example, although speeding is illegal, if a CSIS intelligence officer must exceed posted speed limits to maintain surveillance of a person who is believed to be in the final stages of planning a terrorist attack, such unlawfulness may be justified.

Under new sections 20.1(3) and 20.1(5), the reasonableness of these acts and omissions is to be considered in light of CSIS's information and intelligence collection duties and functions as well as any security threats that may be the object of information and intelligence collection activities or any objectives to be achieved by such activities. The Intelligence Commissioner must review and approve the minister's determination on what classes of acts and commissions are justified.

As set out in sections 20.1(6) and 20.1(7), on the recommendation of the director, the minister may personally designate, respectively, employees who collect information and intelligence and senior employees who have responsibility for these activities, for the purposes of section 20.1 of the CSIS Act. The period of such designations may be no longer than a year.

Under new section 20.1(12), the director or a designated senior employee is empowered to authorize for up to a year, in writing, designated employees to direct the commission of acts and omissions that would otherwise be an offence. To authorize such actions, the director or designated senior employee must believe on reasonable grounds that the acts and omissions are reasonable and proportionate to the threat or to the objective to be achieved, taking into account the reasonable availability of other means to perform the activity or achieve the objective.

New section 20.1(23) stipulates that designated employees who either commit or direct the commission of acts and omissions must submit a written report to the director or a senior designated employee as soon as the circumstances permit.

New section 20.1(8) also provides for the director or a designated senior employee to designate an employee for a period of up to 48 hours under exigent circumstances. The minister must be notified of the designation as soon as the circumstances permit.

2.5.4 Reporting

New section 20.2(1) of the CSIS Act, introduced under clause 101 of the bill, requires CSIS, within three months of the end of the calendar year, to submit to the minister a report on its activities during the preceding year. The minister is to table a copy of the report in both houses of Parliament on any of the first 15 days that each house is sitting after the minister receives it.

Under new section 20.1(24), each year, the minister must issue a public report that includes:

- the number of designations made under exigent circumstances;
- the number of authorizations issued to designated employees to direct the commission of acts and omissions;
- the number of times designated employees directed the commission of acts and omissions under these authorities;
- the nature of the security threats that were the object of information and intelligence collection activities that relied on the commission of acts and omissions; and
- the nature of the acts and omissions that were committed or directed to be committed.

As set out in new section 20.1(25) of the CSIS Act, these reports must not:

- reveal information that would compromise or hinder an ongoing information and intelligence collection activity;
- reveal the identity of an employee acting covertly, a human source, or a person acting covertly under direction;
- endanger the life or safety of an individual;
- prejudice a legal proceeding; or
- be contrary to the public interest.

Under new section 20.1(26) of the CSIS Act, CSIS must notify the NSIRA "as soon as the circumstances permit" after a designation is made under exigent circumstances, a designated employee is authorized to direct the commission of acts and omissions, or a written report is submitted to the director of CSIS or to a designated senior employee describing acts and omissions committed or directed to be committed by a designated employee.

2.6 PART 5: AMENDMENTS TO THE *SECURITY OF CANADA INFORMATION SHARING ACT* (CLAUSES 112 TO 126)

2.6.1 Background

2.6.1.1 General Description of the *Security of Canada Information Sharing Act*

The *Security of Canada Information Sharing Act*[49] (SCISA) was one of the Acts enacted by Bill C-51, the *Anti-terrorism Act, 2015*,[50] which received Royal Assent in June 2015.

Primarily, the SCISA established explicit authorities for information sharing among federal institutions for considerations related to national security. More precisely, the purpose of this act "is to encourage and facilitate the sharing of information among Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada."[51]

Section 5(1) of the SCISA established a new discretionary power for federal institutions to share information in respect of activities that undermine the security of Canada:

> 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 their delegate, if the information is relevant to the recipient institution's jurisdiction or responsibilities under an Act of Parliament or another lawful authority in respect of *activities that undermine the security of Canada*, including in respect of their detection, identification, analysis, prevention, investigation or disruption. [Authors' emphasis]

The concept of a Government of Canada institution is defined in section 2 of the SCISA and includes:

- any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule to the *Privacy Act*; and
- any parent Crown corporation, and any wholly-owned subsidiary of such a corporation, within the meaning of section 83 of the *Financial Administration Act*.

There are 17 recipient Government of Canada institutions, and they are listed in schedule 3 to the SCISA.[52]

2.6.1.2 Reform of the *Security of Canada Information Sharing Act*

2.6.1.2.1 Studies by House of Commons Committees

Two House of Commons committees have conducted studies involving the SCISA in conjunction with the national security consultations launched by the government in September 2016.

In June 2016, the House of Commons Standing Committee on Public Safety and National Security (SECU) undertook a study on Canada's national security framework.[53] In May 2017, it published its report, entitled *Protecting Canadians and their Rights: A New Road Map for Canada's National Security*. The report was accompanied by recommendations, including five for reforms to the SCISA.[54]

In October 2016, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) decided to undertake a study of the SCISA, its effects on privacy since its implementation and amendments that could be proposed during the government's consultations on national security.[55] In May 2017, ETHI published its report, entitled *Safeguarding Canada's National Security While Protecting Canadians' Privacy Rights: Review of the Security of Canada Information Sharing Act (SCISA)*.[56] The report included a number of recommendations for amendments to the SCISA.

2.6.1.2.2 Government of Canada Consultations

In connection with its national security consultations, the Government of Canada published *Our Security, Our Rights: National Security Green Paper, 2016*, which served "to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process."[57] That report contained a section on the sharing of national security information among government institutions, including information sharing subject to the SCISA.

The report on the results of the consultations states that the increased authorities with respect to information sharing between government institutions under the SCISA have raised many concerns. In particular:

> [m]any organizations recommended *SCISA* be repealed or fundamentally revised, with concerns – particularly among human rights, legal and community organizations – that the current definitions of information that can and cannot be shared are too vague and that existing review mechanisms do not provide enough accountability.[58]

With regard to the SCISA, most of the participants in the consultations supported:

- introducing stronger oversight of the SCISA to protect privacy;
- introducing stronger oversight of the SCISA to ensure that recipient government institutions only use information lawfully and in accordance with the rules that apply to those institutions;
- "keeping detailed records of disclosure when sharing information" under the SCISA;
- reducing the number of government institutions that could potentially receive shared information "to those with a core mandate for national security";
- including in the SCISA a more precise definition of "activities of advocacy, protest, dissent and artistic expression";
- clarifying what constitutes an "activity that undermines the security of Canada";
- including in the SCISA a clarification that "institutions receiving national security information must only use that information as permitted by the laws that apply to them, including the *Privacy Act*"; and
- developing "new regulations to require institutions to keep a record of disclosure under *SCISA* to ensure proper accountability."[59]

2.6.2 Bill C-59 Amendments to the *Security of Canada Information Sharing Act*

2.6.2.1 Changes in the English Version of the Act to Replace "Sharing" by "Disclosure" (Clauses 112, 113, 114, 116, 117(1) and 117(3))

The summary of Bill C-59 states that the SCISA is amended to "emphasize that the Act addresses only the disclosure of information and not its collection or use." Accordingly, "information sharing" is replaced by "disclosure of information" or "information disclosure" in a number of places in the English version of the Act, most notably under clauses 112 and 114, in the long and short titles of the Act; under clause 116, in the text describing the purpose of the Act; and under clauses 113, 117(1) and 117(3). The French expression *communication d'information* (and variants of this expression) remains.

2.6.2.2 Preamble (Clause 113(2))

Clause 113(2) of the bill amends the preamble of the SCISA to specify that disclosure of information must respect the *Privacy Act* and other privacy legislation, in addition to the *Canadian Charter of Rights and Freedoms*.

The eighth paragraph of the preamble is amended to state that an explicit authority "will facilitate the effective and responsible disclosure of information to protect the security of Canada."

2.6.2.3 Definitions (Clause 115)

Clause 115 of the bill amends section 2 of the SCISA, which sets out the definitions that apply in the Act.

Clause 115(1) of the bill repeals the definition "people of Canada," which currently reads:

> (a) the people in Canada; or
>
> (b) any citizen, as defined in subsection 2(1) of the *Citizenship Act* – or any permanent resident, as defined in subsection 2(1) of the *Immigration and Refugee Protection Act* – who is outside Canada.

At the same time, clause 115(2) of the bill amends the definition of "activity that undermines the security of Canada" by deleting the term "people of Canada" and by specifying that such activities include activities that threaten the lives or the security of people in Canada or of any individual who has a connection to Canada and who is outside Canada. This therefore includes individuals who are inside Canada regardless of their nationality and individuals with a connection to Canada who are outside the country. The concept of individuals with a connection to Canada is not defined in the bill.

The bill also amends paragraph (a) of the definition of "activity that undermines the security of Canada" to eliminate activities that interfere with the capability of the Government of Canada in relation to the administration of justice, diplomatic or consular relations, or the economic or financial stability of Canada.

Clause 115(4) of the bill amends the SCISA to specify that an activity that undermines the security of Canada includes advocacy, protest, dissent or artistic expression only if any of these activities are carried on in conjunction with an activity that undermines the security of Canada.[60]

2.6.2.4 Guiding Principles (Clause 117(2))

Clause 117(2) of the bill amends the guiding principles set out in section 4 of the SCISA. Specifically, it amends paragraph 4(c) of the SCISA to specify that an information-sharing arrangement is appropriate when a Government of Canada institution regularly discloses information to the same Government of Canada institution.

2.6.2.5 Change to the Authority to Disclose Information (Clause 118)

Clause 118 of the bill amends the threshold for a Government of Canada institution to share information with a recipient Government of Canada institution.

Amended section 5(1)(a) stipulates that the disclosure of information must:

> 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.

In addition, clause 118 adds section 5(1)(b), which requires that the disclosure not affect any person's privacy interest "more than is reasonably necessary in the circumstances."

In various consultations, concerns were raised about the threshold for disclosing information under the Act – that is, relevance – and recommendations were made in this regard. The Privacy Commissioner, SECU and ETHI recommended that the threshold for disclosure provided for in the SCISA be raised from relevance to necessity.[61]

2.6.2.6 Reliability of Information Disclosed

Clause 118 of the bill also amends section 5(2) of the SCISA to include a legal obligation for institutions disclosing information to provide the recipient institution with "information regarding its accuracy and the reliability of the manner in which it is obtained." This amendment responds to this ETHI recommendation: "That the Government of Canada amend the *Security of Canada Information Sharing Act* by creating a legal obligation to ensure the reliability of any shared information."[62]

2.6.2.7 Requirement to Destroy or Return Personal Information

New section 5.1 of the SCISA creates a requirement for government institutions, in certain circumstances, to destroy or return personal information received under the SCISA.

2.6.2.8 Record Keeping (Clauses 119 and 120)

Clause 119(1) adds new section 9(1) to the SCISA to provide a legal obligation for federal institutions that disclose information to keep records containing specific administrative information about the disclosed information. This amendment appears to address the concerns raised that, without records, oversight of the information disclosed under the SCISA is impossible.[63] New section 9(2) contains similar provisions aimed at recipient institutions.

Clause 119(2) of the bill, which adds section 9(3) to the SCISA, provides for an oversight mechanism for the disclosure and receipt of information under the SCISA. Every Government of Canada institution that disclosed or received information during a year must provide the NSIRA with a copy of every record prepared under sections 9(1) and 9(2) within 30 days of the end of the year. Unless a regulation is made under section 9(1)(f) of the SCISA or clause 120 of the bill, the oversight will apparently not cover the recipient information.

The bill also amends section 10 of the SCISA to authorize the making of regulations to keep the records described in section 119(1) of the bill.

2.7 PART 6: AMENDMENTS TO THE *SECURE AIR TRAVEL ACT* (CLAUSES 127 TO 139)

2.7.1 Background

Transport Canada established the Passenger Protect Program and its associated "Specified Persons List" (SPL) in June 2007, following the enactment in 2004 of the *Public Safety Act, 2002*.[64] That Act resulted in numerous amendments to the *Aeronautics Act*,[65] including the enactment of section 4.81(1), which authorizes the Minister of Transport to require that air carriers disclose information on "any particular person specified by the Minister." This information, when disclosed, is consolidated into the SPL.

The *Anti-terrorism Act, 2015* broadened the Passenger Protect Program by enacting the *Secure Air Travel Act* (SATA),[66] which replaced the previous regime under which specified persons were listed. The SATA, in section 8(1), established a legislative framework authorizing the Minister of Public Safety and Emergency Preparedness to establish a list of persons (the SPL, commonly referred to as the "no-fly list") for whom there are reasonable grounds to suspect that they:

- will engage or attempt to engage in an act that would threaten transportation security; or

- will travel by air for the purpose of committing a specified terrorism offence (participation in the activities of a terrorist group, facilitating terrorist activity or the commission of an offence for a terrorist group) or an indictable offence where the act or omission involved also constitutes a terrorist activity,[67] inside or outside of Canada.

Concerns were raised by Canadians with respect to the efficacy of the Passenger Protect Program, the listing of persons, the number of false positives, the lack of a redress mechanism and the need to strengthen the administrative recourse and appeal provisions within SATA. These and other issues were brought to light during the Government of Canada's public consultations on national security launched in 2016 and the parallel study conducted by SECU.[68]

2.7.2 Specified Persons List (Clause 129)

Clause 129 of the bill amends current section 8 of SATA in order to ensure the inclusion of the middle names of individuals on the SPL, as well as any other information prescribed by regulation that would serve to identify the individuals.

2.7.3 Duty of Air Carriers and the Sharing of Passenger Information (Clause 127)

The SATA currently requires air carriers or operators of an aviation reservation system to provide any of the passenger information enumerated in the schedule to the *Aeronautics Act*[69] concerning persons who are on board or expected to be on board an aircraft for any flight. The passenger information is then collected by the Canada Border Services Agency (CBSA) and compared to information on the SPL in order to identify a listed person who is attempting to travel. Under current section 14 of SATA, the CBSA can then disclose to air carriers and operators of aviation reservation systems that a passenger's name is the same as that of a listed person.

Clause 127 of Bill C-59 amends section 6(2) of SATA to mirror the changes made to section 8. Consequently, an air carrier must also provide the middle names of individuals and any other information that is prescribed by regulation, if such information is in their control. The other listed items are the first name and surname of individuals, their date of birth and gender. The time and manner for the delivery of the information will be prescribed by regulation.

Moreover, new section 6(4) of SATA modifies the legal framework requiring air carriers and operators of an aviation reservation system to provide information in their control to either the Minister of Public Safety and Emergency Preparedness or the Minister of Transport upon request. The scope of the duty to provide information upon request is limited to the enumerated passenger information set out in the schedule to the *Aeronautics Act*, but it can be expanded to include other information prescribed by regulation. Under new section 6(5), the requested information can only be in respect of a listed person, or one who is believed to be listed.

Current section 10 of SATA provides a framework for assistance to the Minister of Public Safety and Emergency Preparedness by the following authorities:

> (a) the Minister of Transport;
>
> (b) the Minister of Citizenship and Immigration;
>
> (c) a member of the Royal Canadian Mounted Police or a civilian employee of that police force;
>
> (d) the Director or an employee of the Canadian Security Intelligence Service;
>
> (e) an officer or employee of the Canada Border Services Agency; and
>
> (f) any other person or entity prescribed by regulation.

New section 6(6) of SATA limits the scope of the information that can be requested by the persons listed in sections 10(b) to 10(f) of SATA, giving them the authority to request from the air carriers only information that is listed in the schedule to the *Aeronautics Act*[70] or that is prescribed by regulation. Again, the requested information can only be for a person who is listed or believed to be listed and for the sole purpose of assisting the Minister of Public Safety and Emergency Preparedness in the administration and enforcement of SATA.

2.7.4 Collection and Disclosure of Information (Clause 130)

2.7.4.1 Unique Identifier (Pre-flight Verification of Identity)

Clause 130 of the bill, in new section 10.1 of SATA, introduces the notion of a "unique identifier" within the legal framework of SATA. The Minister of Public Safety and Emergency Preparedness may, for the purpose of issuing a unique identifier to travellers in order to assist with the verification of their identity before a flight, collect any personal information provided by the travellers.

2.7.4.2 Collection of Passenger Information for Identification Purposes

To identify listed persons on board, or expected to be on board, an aircraft, clause 130 of the bill, through new section 10.2 of SATA, grants the Minister of Public Safety and Emergency Preparedness the authority to collect passenger information provided or deemed to have been provided under new sections 6(2), 6(3) and 6(4).

As previously noted, under section 10, SATA continues to provide a framework for sharing the collected passenger information between federal departments and agencies, namely Transport Canada; Public Safety Canada; Immigration, Refugees and Citizenship Canada; the RCMP; CSIS; and the CBSA.

2.7.4.3 Disclosure of Information

As noted above, the legislative framework for the disclosure of information is broadened by new sections 6(2) and 6(3) of SATA. New section 10.3 of SATA, which permits the authorized disclosure of passenger information obtained or deemed to have been obtained from air carriers, empowers the minister to:

- disclose information for the purpose of obtaining assistance in identifying listed persons who are on board or expected to be on board an aircraft, if the information relates to a person whom the minister has reason to believe is a listed person; and
- disclose information in order to comply with a subpoena or document issued or an order made by a court, person or body with jurisdiction to compel the production of information or to comply with rules of a court relating to the production of information.

New section 10.3(2) states that the Minister of Public Safety and Emergency Preparedness continues to have the authority to disclose information for the purposes of transportation security or the prevention of travel by air for the purpose of engaging in terrorist activity, as defined in current section 8(1)(b) of SATA. If the information relates to a listed person, it must have been obtained from, or deemed to have been provided by, the air carriers under new sections 6(2) and 6(3) of SATA.

Moreover, new section 11 of SATA states that the minister continues to have the authority to disclose information obtained in the exercise or performance of his or her powers, duties or functions under the Act for the purposes of transportation security or the prevention of travel by air for the purpose of engaging in terrorist activity, as long as it is not information provided under section 6(2) or section 6(3).

Subject to written agreements, new section 12 of SATA provides that the minister may disclose "any information that he or she is, under section 10.3(2) or section 11, permitted to disclose" and may also disclose the SPL, in whole or in part, to a government of a foreign state, an institution of such a government or an international organization. The latter disclosure power was already provided to the minister under current section 12 of SATA.

New section 12.1 of SATA provides that the minister may disclose to a child's parent, guardian or tutor that the child is not a listed person.

2.7.5 Canada Border Services Agency Disclosure Powers (Clause 133)

Clause 133 of Bill C-59 eliminates the previously mentioned power of the CBSA to disclose to air carriers and operators of aviation reservation systems that the name of a passenger is the same as that of a listed person. Under amended section 14 of SATA, the CBSA is only authorized to disclose to the Minister of Public Safety and Emergency Preparedness (or any other person or entity referred to in section 10) information that is collected from air carriers and operators of aviation reservation systems about a listed person or about a person whom the Minister of Public Safety and Emergency Preparedness or the Minister of Transport, believing that person to be a listed person, has informed the CBSA of that belief.

2.7.6 Exemption Powers (Clause 128)

New section 7.1(1) of SATA provides that the Minister of Public Safety and Emergency Preparedness may order that an air carrier be exempted from its duty to provide passenger information as specified in new section 6(2) of SATA or in regulations if, in the minister's opinion:

> (a) the urgency of a situation or circumstances beyond the air carrier's control would make it difficult for it to comply with that subsection or provision; and
>
> (b) the exemption is not likely to adversely affect transportation security.

Furthermore, new section 7.2 provides the minister with the authority to exempt an air carrier or a class of air carriers from the application of a provision of the regulations to allow for the "conduct of tests, including tests of new kinds of technologies and tests of alternative measures to those set out in the provision" in order to allow the minister "to determine whether any changes to the regulations are required as a result, if, in his or her opinion, the exemption is not likely to adversely affect transportation security."

2.7.7 Information Destruction (Clause 136)

Under clause 136 of the bill, section 18 of SATA is rewritten to expressly provide that despite any other Act of Parliament, including the *Access to Information Act* and the *Privacy Act*,[71] both the Minister of Public Safety and Emergency Preparedness and the Minister of Transport, under new sections 18(1) and 18(2) of SATA respectively, are required to destroy, within seven days of the day on which the flight either departs or is cancelled, any document or record about a person who is or was on board or expected to be on board the aircraft, unless the information (provided or disclosed pursuant to sections 6(2) to 6(4) and 13(d)) is reasonably required for the purposes of the Act.

Clause 136 of Bill C-59, through new section 18(3) of SATA, also provides that all other persons and entities referred to in section 10 of SATA are bound by the information destruction requirement. This would include the Minister of Citizenship and Immigration, the RCMP, CSIS, the CBSA and any other person or entity specified by regulation.

Clause 136 of Bill C-59 amends section 19 of SATA to provide that nothing in the Act limits or prohibits the lawful retention of information, in addition to the exiting provision for the collection, use and disclosure of information. In other words, the federal department and agencies providing assistance to the Minister of Public Safety and Emergency Preparedness (by way of section 10 in SATA), which are lawfully authorized to collect, use and disclose information, can lawfully retain information, if they have the statutory authority to do so.

By way of example, SATA would not hinder CSIS's ability to retain information that it is lawfully authorized to collect, use, disclose or retain under the CSIS Act. The interpretive framework provided within section 19 of SATA appears to reflect the terminology and reasoning behind the 2016 Federal Court decision concerning the retention of metadata by CSIS, and its indication that the mandate and functions of CSIS must be strictly defined and limited.[72]

2.7.8 Administrative Recourse (Clause 134)

Under SATA, a listed person may apply to have his or her name removed from the SPL within 60 days of being denied transportation.[73] The individual must be afforded a reasonable opportunity to make representations. The Minister of Public Safety and Emergency Preparedness must then decide whether reasonable grounds to maintain the applicant's name on the list continue to exist and, without delay, give the applicant notice of any decision (but not the reasons for it) made in respect of the application. If the minister does not make a decision about the application within 90 days, or within any further period that is agreed on by the minister and the applicant, the minister is deemed to have denied it.

Amended section 15(6) grants the minister 30 days in addition to the original 90 days after the day on which the application is received, for a total of 120 days. If the minister has insufficient information to make a decision and notifies the applicant within that 120 days, the period may be extended by 120 days. In contrast to the existing presumption in SATA, Bill C-59 states that upon expiry of the period, "the Minister is deemed to have decided to remove the applicant's name from the list." SECU made a similar recommendation.[74]

2.7.9 Right to Appeal (Clause 135)

SATA affords a listed person the right to appeal to the Federal Court in respect of any ministerial direction made under section 9 of the Act and any ministerial decision to add or retain the person's name on the list made under section 8 or section 15 of the Act.

A listed person who has been denied transportation as a result of a direction made under section 9 may commence an appeal only after having been denied the removal of his or her name from the SPL as a result of the administrative recourse provided for in section 15 of the Act. Section 16 states that there is a 60-day appeal period.

Clause 135 of Bill C-59 amends section 16(2) of SATA in order to reflect both the changes made to the administrative recourse provisions and the deletion of the reference to the minister's deemed decision brought under section 15(6) of SATA. An appeal may be launched within 60 days of the day on which the notice of the minister's decision, referred to under current section 15(5) of SATA, is received. The bill does not remove the right of appeal of a direction made under section 9 of SATA and any decision made by the minister under section 15.

Of note, Bill C-59 does not modify the existing appeal procedures in SATA, which are very similar to those set out in the pre-2008 *Immigration and Refugee Protection Act* (IRPA) process for the review of security certificates and detention orders. The Supreme Court of Canada in *Charkaoui v. Canada (Citizenship and Immigration)* examined this process and found that the IRPA scheme was in violation of the right to life, liberty and security of the person, and the right not to be deprived of those rights except in accordance with the principles of fundamental justice guaranteed under section 7 of the Charter.[75]

Although an individual on the SPL may submit a delisting application to the Chief Justice of the Federal Court,[76] that individual will not have access to confidential documents, and the procedure provided for in SATA – unlike the security certificates procedure in the *Immigration and Refugee Protection Act* – does not allow for special advocates.[77]

In such appeals, the Federal Court must review whether the decision is reasonable on the basis of the information available. As set out in section 16(6)(e), the usual rules of evidence do not apply to the appeal proceeding, as SATA allows for the admission of hearsay evidence: "the judge may receive into evidence anything that, in the judge's opinion, is reliable and appropriate, even if it is inadmissible in a court of law, and may base a decision on that evidence." Sections 16(6)(a) to 16(6)(c) state that:

> a) at any time during a proceeding, the judge must, on the request of the Minister, hear information or other evidence in the absence of the public and of the appellant and their counsel if, in the judge's opinion, its disclosure could be injurious to national security or endanger the safety of any person;
>
> b) the judge must ensure the confidentiality of information and other evidence provided by the Minister if, in the judge's opinion, its disclosure would be injurious to national security or endanger the safety of any person; and
>
> c) throughout the proceeding, the judge must ensure that the appellant is provided with a summary of information and other evidence that enables them to be reasonably informed of the Minister's case but that does not include anything that, in the judge's opinion, would be injurious to national security or endanger the safety of any person if disclosed.

Ultimately, the judge may base a decision on information or other evidence even if a summary of that information or other evidence has not been provided to the appellant.

In its report *Protecting Canadians and their Rights: A New Road Map for Canada's National Security*, SECU recommended that SATA be amended in order to provide for the nomination of a special advocate to protect the interest of individuals who have appealed to have their name removed from the SPL. SECU commented on the extent of the intrusions on the liberty and security of individuals resulting from the operation of the appeal provisions and called for increased fairness, openness and transparency. Moreover, SECU recommended that Public Safety Canada's annual report to Parliament should include the number of individuals on the SPL.[78] Bill C-59 does not respond to these recommendations.

2.8 PART 7: AMENDMENTS TO THE *CRIMINAL CODE* (CLAUSES 140 TO 154)

2.8.1 Background

As part of its national security consultations, the Government of Canada's document *Our Security, Our Rights: National Security Green Paper, 2016* looked at the anti-terrorism measures set out in the *Criminal Code*. The document explains that Bill C-51, the *Anti-terrorism Act, 2015* amended the *Criminal Code* to:

> a) make it easier to prevent the carrying out of terrorist activity or terrorism offences;
> b) make it a crime to advocate or promote terrorism offences;
> c) give courts the power to order the seizure and forfeiture or removal of terrorist propaganda; and
> d) give additional protection to witnesses and other participants in national security proceedings.[79]

The report on the results of the consultations, *National Security Consultations: What We Learned Report*, published in March 2017, had this to say about the *Criminal Code*:

- The majority of participants expressed concerns that the amendments made to the *Criminal Code* by the *Anti-terrorism Act, 2015* "could lead to a loss of personal liberties and infringe on freedom of expression."[80]
- Two-thirds of participants stated that "the thresholds for obtaining recognizance with conditions and terrorism peace bonds" were inappropriate and did not "strike the correct balance between national security and protecting the rights of individuals."[81]
- "[A]lmost half (47%) of online responses say the advocacy offence should be clarified so that it more clearly resembles the existing offence of counselling."[82]
- The majority of participants felt that the definition of "terrorist propaganda" was "too broad and could lead to the conviction of innocent people."[83]

The government green paper also discussed the procedures set out in the *Criminal Code* for listing terrorist entities. On that topic, the "What We Learned" report on the results of the national security consultations stated that 52% of participants felt that "the current listing methods meet Canada's domestic needs and international obligations"[84] and that 44% thought they did not. Some 62% of participants said that:

> current safeguards do not provide an adequate balance between national security and protecting the rights of Canadians and [they] offered several suggestions for improving the safeguards, ranging from clarifying the definition of "terrorism" and the criteria for adding a group or individual to the list, making the list public, creating an appeal process and mandating more independent oversight.[85]

In its 2017 report entitled *Protecting Canadians and their Rights: A New Road Map for Canada's National Security*, SECU included recommendations on ways to reform the anti-terrorism measures in the *Criminal Code*.[86]

2.8.2 List of Terrorist Entities Provided for in Section 83.05 of the *Criminal Code*

2.8.2.1 Current System

In 2001, the *Anti-terrorism Act* enacted new provisions of the *Criminal Code* providing for a list of entities involved in terrorist activities.[87] The *Criminal Code* establishes the procedure for placing an entity on, and removing it from, the list. The term "entity" is defined as "a person, group, trust, partnership or fund or an incorporated association or organization."[88]

In general, the Governor in Council is allowed to establish a list by regulation.[89] Under section 83.05(1) of the *Criminal Code*, the Governor in Council may include:

> any entity if, on the recommendation of the Minister of Public Safety and Emergency Preparedness, the Governor in Council is satisfied that there are reasonable grounds to believe that
>
> > (a) the entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or
> >
> > (b) the entity is knowingly acting on behalf of, at the direction of or in association with an entity referred to in paragraph (a).

The main consequences of the system for listing entities involved in terrorist activities are the following:

- While "[i]t is not a crime to be listed," placement on the list is "a public means of identifying a group or individual as being associated with terrorism."[90]
- An entity placed on the list is automatically considered a "terrorist group" within the meaning of the *Criminal Code*. In fact, it is important to note that the definition of "terrorist group" in section 83.01(1) of the *Criminal Code* includes entities placed on the list established by the Governor in Council under section 83.05 of the *Criminal Code*. The term "terrorist group" is used in a number of places in the *Criminal Code*, including to establish terrorism-related offences (see, for example, section 83.18 of the *Criminal Code* concerning participation in the activity of a terrorist group). In short, when an entity is placed on the list, it is not necessary to prove that one of its objects or activities is to engage in or facilitate terrorist activities.[91]

- Listed entities may see their goods frozen, seized or confiscated under sections 83.08 and following of the *Criminal Code*.[92] As described by Public Safety Canada, section 83.11 of the *Criminal Code* states that certain institutions, such as banks, "are subject to reporting requirements with respect to an entity's property and must not allow those entities to access the property."[93]

2.8.2.2 Amendments to the Procedure for Including and Removing Listed Entities Involved in Terrorist Activities (Clauses 141 and 142)

Clause 141 of Bill C-59 amends certain rules set out in the *Criminal Code* regarding the procedure for listing entities involved in terrorist activities.

Under new section 83.05(1.2)(a) of the *Criminal Code*, added by clause 141(2) of the bill, the Minister of Public Safety and Emergency Preparedness is authorized, if he or she has reasonable grounds to believe that a listed entity is using a name that is not on the list:

- to change the name of the entity on the list; or
- to add any other name to the list.

This new provision apparently reduces the burden of proof when adding the name of an entity linked to an entity already on the list, since, as mentioned earlier, at present an entity may be placed on the list under section 83.05(1) of the *Criminal Code* if there are reasonable grounds to believe that the entity "has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity" or "is knowingly acting on behalf of, at the direction of or in association with an entity."

Similarly, under new section 83(1.2)(b) of the *Criminal Code*, the minister is authorized to delete from the list any name by which a listed entity may have been known but which it no longer uses.

Under new section 83.05(3) of the *Criminal Code*, the deadline for rendering a decision on an application by a listed entity to have its name deleted from the list increases from 60 to 90 days. If the minister has not made a decision within that time (or within a longer period agreed upon by the minister and applicant), the minister is deemed to have decided that the applicant should remain a listed entity.

Clause 141 of the bill amends the rules governing the periodic review of the list by the minister to determine whether an entity's inclusion on the list is still justified. New section 83.05(8.1) of the *Criminal Code* provides for a review of the entities on the list every five years. The current review period is two years (section 83.05(9) of the *Criminal Code*). Under new section 83.05(10), the minister must publish a notice of the results of the review in the *Canada Gazette* in the five years following the

conclusion of the review. At the moment, section 83.05(10) of the *Criminal Code* provides that the results of the review must be published in the *Canada Gazette* without delay.

2.8.3 Counselling Commission of Terrorism Offence (Clause 143)

The *Anti-terrorism Act, 2015* (former Bill C-51) created section 83.221 of the *Criminal Code*, which concerns advocating or promoting commission of terrorism offences in general.

During his appearance before SECU in March 2015 during the study of Bill C-51, the Honourable Peter MacKay, then Minister of Justice and Attorney General of Canada, explained that new section 83.221 filled a gap:

> Currently it's a crime to counsel someone to commit a specific crime like murder. It is not a crime, however, to counsel somebody to commit a broad category of criminal activity like terrorism, one lacking specific detail as to which offence is being encouraged to be committed. Therefore, the focus of the proposed new offence is to cover the situation where the active encouragement lacks the specific detail that would link the encouragement to the commission of a specific terrorism offence, although in the circumstances it is clear that someone is actively encouraging to commit any of the terrorism offences in the *Criminal Code*. In other words, it would not matter whether a specific terrorism offence is advocated or promoted for criminal liability to attach. To be clear, this is not a glorification of terrorism offence.[94]

It should be noted that the SECU report on national security tabled in May 2017 indicated that there were criticisms of the scope of section 83.221 of the *Criminal Code.* According to a number of witnesses,

> this new offence is unconstitutional as it is vague, too broad and an unreasonable restraint on the freedom of expression. For such an offence to be legitimately prohibited, there must be a very close nexus between a statement and the risk of harm.[95]

Clause 143 of the bill amends section 83.221 of the *Criminal Code*. The changes are listed in Table 1.

Table 1 – Bill C-59 Amendments to Section 83.221 of the *Criminal Code*
(Advocating or promoting commission of terrorism offences)

Section 83.221 Currently in Force	Section 83.221 in Bill C-59
83.221(1) Every person who, by communicating statements, knowingly advocates or promotes the commission of terrorism offences in general – other than an offence under this section – while knowing that any of those offences will be committed or being reckless as to whether any of those offences may be committed, as a result of such communication, is guilty of an indictable offence and is liable to imprisonment for a term of not more than five years. (2) The following definitions apply in this section. *communicating* has the same meaning as in subsection 319(7). *statements* has the same meaning as in subsection 319(7).	83.221(1) Every person who counsels another person to commit a terrorism offence without identifying a specific terrorism offence is guilty of an indictable offence and is liable to imprisonment for a term of not more than five years. (2) An offence may be committed under subsection (1) whether or not a terrorism offence is committed by the person who is counselled.

The terms currently used in section 83.221 of the *Criminal Code* – "by communicating statements, knowingly advocates or promotes the commission of terrorism offences in general" – are similar to those used in sections 318 and 319, which establish the offences related to hate propaganda. It should be noted that specific defences are provided for in section 319(3) of the *Criminal Code* for the offence of voluntarily promoting hate propaganda under section 319(2) of that Act. However, such defences are not provided for in section 83.221 of the *Criminal Code*. Moreover, some of the witnesses who appeared before SECU during its study of the National Security Framework:

> queried why the new offence does not include similar defences to the ones provided for the offence of promoting hatred or, simply, why other offences – such as encouraging participation in an activity of a terrorist group or instructing a person to carry out an activity for a terrorist group – are inadequate.[96]

In addition, the terms used in new section 83.221 – "counsels another person to commit a terrorism offence" – are similar to the terms used for the offence of counselling an offence provided for in section 22 of the *Criminal Code*. However, the *Criminal Code* provides no specific defence to the offence of counselling.

Finally, section 83.221 of the *Criminal Code* in its current form makes it an offence to advocate or promote the commission of "terrorism offences in general" by communicating statements. New section 83.221 makes it an offence to counsel another person to commit "a terrorism offence without identifying a specific terrorism offence." The practical difference between the descriptions of the offences is not clear.

2.8.4 Terrorist Propaganda (Clause 144)

The *Criminal Code* provides for the issuance of warrants to seize and confiscate publications or erase electronic data on a computer that constitute "terrorist propaganda."

Clause 144 of the bill amends the definition of "terrorist propaganda" set out in section 83.222(8) of the *Criminal Code* to reflect the new language to describe the new offence of counselling the commission of a terrorist offence.

2.8.5 Preventive Measures

Currently, the *Criminal Code* provides for various measures designed to prevent the commission of acts of terrorism:

- investigations before a judge (sections 83.28 and 83.29);
- preventive arrest without a warrant and detention for a maximum of one week (section 83.3(4));
- recognizance with conditions (section 83.3(8)); and
- sureties to keep the peace when a person fears that another person may commit a terrorism offence (section 810.011).

These measures often attract criticism.

2.8.5.1 Investigative Hearings (Clauses 145 and 147)

Bill C-59 eliminates investigative hearings before a judge. The investigative hearing for the Air India affair[97] is the only time this special procedure was used.

2.8.5.2 Arrest Without Warrant and Recognizance with Conditions (Clauses 146 and 148)

A recognizance with conditions can be used when the police suspect someone is connected in some way to the carrying out of a terrorist activity. For example, if the RCMP suspect that someone is connected to a broad plot to attack a train station but do not know the individual's exact role, they can use a terrorism peace bond to prevent the individual from committing a specific terrorism offence, such as using explosives or attempting to leave Canada to join a terrorist group.

Bill C-59, under new sections 83.3(2)(b) and 83.3(4), raises the threshold at which a terrorism suspect can be arrested without a warrant, and a recognizance with conditions can be obtained, as set out in section 83.3 of the *Criminal Code*. This threshold was lowered by the *Anti-terrorism Act, 2015* in order to facilitate police access to these exceptional procedures.

New section 83.32(1) extends the validity of section 83.3 to five years after the coming into force of Bill C-59. Under the current rules, this section was to have automatically ceased to have effect on the 15th sitting day after 15 July 2018 unless Parliament, after conducting a comprehensive review, passed a resolution authorizing its extension.

It should be noted that, since these measures were created in 2001, the police have used neither arrest without a warrant nor recognizance with conditions.

2.8.5.3 Sureties to Keep the Peace (Clause 153)

New section 810.011(15) of the *Criminal Code* requires the Attorney General of Canada to produce a report on the number of recognizances entered into each year under section 810.011.

It should be noted that the sureties to keep the peace provided for in section 810.011 are frequently used by police. That is probably why Bill C-59 includes a provision on oversight of these recognizances.

2.8.6 Protection of Witnesses (Clause 154)

Another issue that is regularly raised with respect to terrorism trials is the protection of witnesses.

Section 486 and following of the *Criminal Code* provide for rules governing the protection of witnesses. For example, section 486 allows the court to exclude the public or to authorize a person to testify from behind a screen, and section 486.7 of the *Criminal Code* authorizes a tribunal to allow a person to testify anonymously.

New section 810.5 allows the court to issue the witness protection orders provided for in sections 486 to 486.5 and 486.7 of the *Criminal Code* for the recognizance procedures provided for in sections 83.3 and 810 to 810.2.

2.9 PART 8: AMENDMENTS TO THE *YOUTH CRIMINAL JUSTICE ACT* (CLAUSES 159 TO 167)

The *Youth Criminal Justice Act* (YCJA),[98] which came into force in 2003, creates a criminal justice system separate from the one for adults, based on the principle that the moral culpability of young people is not as great. The YCJA applies when a young person between the ages of 12 and 17 is involved in an offence created by federal legislation (such as the *Criminal Code*) and its regulations. The YCJA also creates youth courts.

2.9.1 Application of Protections for Youth (Clauses 159 to 164)

The YCJA indicates that the youth criminal justice system is intended to protect the public "through measures that are proportionate to the seriousness of the offence and the degree of responsibility of the young person" while providing for special rules intended to guarantee the rights and freedoms of young people.[99]

New section 14(2) of the YCJA, provided in clause 159 of the bill, expressly states that the principles and guarantees of the YCJA apply to the preventive anti-terrorism measures set out in sections 83.3 and 810.011 of the *Criminal Code*. New section 29(1) of the YCJA, in clause 163 of the bill, contains a stipulation that the principle that detention is not a substitute for social measures (such as mental health and youth protection measures) applies to the preventive detention provided for in section 83.3 of the *Criminal Code*. New section 30(1) of the YCJA, set out in clause 164 of the bill, stipulates that young people must be detained in a safe, fair and humane manner.

New sections 25(3)(a) and 25(3)(a.1) of the YCJA, found in clause 161 of the bill, set out that a youth court is required to inform young people affected by a preventive anti-terrorism measure of their right to obtain counsel.

2.9.2 Access to Young People's Records for the Purposes of the Canadian Passport Order (Clause 167)

The YCJA, in section 3(1)(b), states that "the criminal justice system for young persons must be separate from that of adults, must be based on the principle of diminished moral blameworthiness or culpability and must emphasize," among other things, "enhanced procedural protection to ensure that young persons are treated fairly and that their rights, including their right to privacy, are protected." Indeed, since the *Juvenile Delinquents Act* of 1908:

> the Canadian youth justice system has operated on the principle that publishing the identity of a young person would adversely affect his or her reintegration into society, would be prejudicial to him or her and, therefore, would compromise long-term public safety.[100]

The general rule, therefore, articulated in section 110 of the YCJA, is that information relating to the identity of a young person is not published. The rules governing record keeping by Canadian courts, police, and government departments and agencies are set out in sections 114 to 116 of the YCJA. In sections 117 and following, the YCJA also includes rules restricting access to young people's records. In general, as set out in section 118, access to young people's records is prohibited.

More specifically, section 119 of the YCJA designates those individuals – such as parents, victims, judges and prosecutors – who can access a young person's records. This section also sets a specific time limit for access to certain information in a record. Once that time limit has expired, access to the record is no longer authorized.

Clause 167(1) of Bill C-59 adds a new paragraph to section 119(1) of the YCJA such that "an employee of a department or agency of the Government of Canada, for the purpose of administering the *Canadian Passport Order*" is included among "persons having access to records" under the YCJA. The *Canadian Passport Order* concerns the issuance of passports, refusal to issue passports, revocation of passports and the cancellation of passports.[101]

At present, section 119(2) of the YCJA does not provide for a time limit on access to the records of young people covered by orders made under section 14(2) of the YCJA (such as orders concerning a recognizance related to terrorist activities [section 83.3 of the *Criminal Code*]) and under section 20(2) of the YCJA (recognizance – fear of injury or damage [section 810 of the *Criminal Code*]). Clause 167(2) of Bill C-59, in new paragraph 119(2)(d.1) of the YCJA, places a limit of six months on access to the records of young people covered by an order made under sections 14(2) and 20(2) of the YCJA.

NOTES

1. Bill C-59, An Act respecting national security matters, 1st Session, 42nd Parliament.
2. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, 1977–1981.
3. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*, 2006; and Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Arar Commission Factual Inquiry*.
4. Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, *Final Report*.
5. Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy*, Final Report, 2010.
6. Bill C-51, An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts, 2nd Session, 41st Parliament (S.C. 2015, c. 20) [*Anti-terrorism Act, 2015*]. See also Julie Béchard et al., *Legislative Summary of Bill C-51: An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, Publication no. 41-2-C51-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 19 June 2015.
7. Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016*, 2016.
8. Hill and Knowlton Strategies, *National Security Consultations: What We Learned Report*.

9. *National Security and Intelligence Committee of Parliamentarians Act*, S.C. 2017, c. 15. See also Holly Porteous and Dominique Valiquet, *Legislative Summary of Bill C-22: An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts*, Publication no. 42-1-C22-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 22 August 2016.

10. See the summary of the evidence given in connection with the study and report by House of Commons Standing Committee on Public Safety and National Security [SECU], *Protecting Canadians and their Rights: A New Road Map for Canada's National Security*, Ninth Report, 1st Session, 42nd Parliament, May 2017.

11. *Security of Information Act*, R.S.C. 1985, c. O-5.

12. That said, the principle of "originator control" could see foreign allies exercising their right to block access by the National Security and Intelligence Review Agency. Caveats prohibiting further dissemination without the originator's consent are a form of originator control. See reference to "originator control" in clause 117 of the bill, which amends section 4 of the *Security of Canada Information Sharing Act*.

13. *National Defence Act*, R.S.C. 1985, c. N-5.

14. *Inquiries Act*, R.S.C. 1985, c. I-11.

15. *Royal Canadian Mounted Police Act*, R.S.C. 1985, c. R-10.

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

17. *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17.

18. The provisions of the *Security of Canada Information Disclosure Act* are contained in Part 5 of Bill C-59 and are discussed in section 2.6 of this Legislative Summary.

19. *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23.

20. *Financial Administration Act*, R.S.C. 1985, c. F-11.

21. *Public Service Employment Act*, S.C. 2003, c. 22, ss. 12, 13.

22. This formulation includes superior and appellate courts in each province, but excludes the Supreme Court of Canada, the Federal Court, the Federal Court of Appeal, and provincial courts.

23. Department of Justice, *Charter Statement – Bill C-59:* An Act respecting national security matters, 20 June 2017.

24. Decisions of the Intelligence Commissioner would presumably be subject to judicial review under the *Federal Courts Act*. The judicial review powers of the Federal Court apply to all federal boards, commissions or other tribunals, defined as:

> any body, person or persons having, exercising or purporting to exercise jurisdiction or powers conferred by or under an Act of Parliament or by or under an order made pursuant to a prerogative of the Crown, other than the Tax Court of Canada or any of its judges, any such body constituted or established by or under a law of a province or any such person or persons appointed under or in accordance with a law of a province or under section 96 of the *Constitution Act, 1867*.

See *Federal Courts Act*, R.S.C. 1985, c. F-7, s. 2(1).

25. Section 4 of the Communications Security Establishment (CSE) Act raises the possibility of another minister being designated responsibility for CSE.

26. It should be noted that under the proposed CSE Act (discussed in section 2.4 of this Legislative Summary), CSE will be empowered to engage in five classes of activity, each of which will require ministerial authorization. However, only foreign intelligence collection and cybersecurity activities will require validation by the Intelligence Commissioner.

27. See sections 26, 27 and 29 of the CSE Act, found in clause 76 of Bill C-59.

28. Facial recognition software is increasingly being used for border control and counter-terrorism purposes.

29. For example, the Internet is built to be redundant and adaptable in the face of localized outages and traffic surges. Thus, a communication sent over the Internet might pass through one set of routers one day and use a completely different set the next.

30. One reason why CSE might need to acquire information in this manner would be to discover and characterize how its foreign intelligence targets interact with the global information infrastructure.

31. *Criminal Code*, R.S.C. 1985, c. C-46.

32. See Jordan Press, The Canadian Press, "Top courts threaten federal government with legal action over new IT rules," *Globe and Mail*, 16 May 2018. See also Amanda Connolly, "CSE chief says federal departments need to 'get on' Shared Services' cyber defences," *iPolitics*, 21 March 2016.

33. Some observers have suggested that CSE might use "human agents to modify software, implant physical devices, or otherwise assist in the collection of foreign intelligence." See Bill Robinson, "CSE and Bill C-59 overview," *Lux Ex Umbra*, Blog, 4 August 2017.

34. *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11.

35. Operational since December 2016, the Canadian Cyber Threat Exchange is a not-for-profit organization that, for an annual $50,000 membership fee, provides critical infrastructure owners and operators with access to shared cyber threat information, including "tear-lined" CSE information. In intelligence reporting, "below the tear line" information is information that has been sanitized and approved for disclosure. For example, in threat intelligence shared with the private sector, CSE would likely remove any information revealing sources and methods used to obtain the intelligence. This is possible to achieve using automated means. To read more, see "The Canadian Cyber Threat Exchange (CCTX) is operational and reaching out to Canadian businesses," *Canadian News Wire*, 9 December 2016; and Canadian Cyber Threat Exchange, *Frequently Asked Questions*.

36. Section 34(2)(c) of the CSE Act states that:

> (2) The Minister may issue an authorization under subsection 26(1) [foreign intelligence authorizations] only if he or she concludes that there are reasonable grounds to believe – in addition to the matters referred to in subsection (1) – that …
>
> > (c) the measures referred to in section 24 will ensure that information acquired under the authorization that is identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential to international affairs, defence or security.

In its discussion of section 33, the Charter Statement for Bill C-59 mentions:

> Further, no activities directed at Canadians or persons in Canada could be authorized; only activities aimed outside Canada at foreign individuals, entities and the GII [global information infrastructure] outside of Canada would be permitted.

See Department of Justice (2017).

37. The *Criminal Code*, section 2, defines "bodily harm" as "any hurt or injury to a person that interferes with the health or comfort of the person and that is more than merely transient or trifling in nature."

38. See, for example, Office of the CSE Commissioner, "Proposed amendments to the *National Defence Act*," *Annual Report 2007–2008*, 2008, p. 4; and Office of the CSE Commissioner, "Review of CSE foreign signals intelligence metadata activities (Part 2)," *Annual Report 2015–2016*, 2016, pp. 20–22. See also Office of the Privacy Commissioner of Canada, "Recommendations for Improvement," *Special Report to Parliament – Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance*, 28 January 2014, recommendation 9; and Office of the Privacy Commissioner of Canada, "Privacy and Canada's national security framework," Backgrounder, 6 December 2016.

39. Owen Bowcott, "UK intelligence agencies face surveillance claims in European court," *The Guardian* [London], 7 November 2017.

40. United Kingdom, Investigatory Powers Tribunal, *Privacy International vs. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and Secret Intelligence Service*, [2016] UKIPTrib 15_110-CH, para. 7(48).

41. Department of Justice (2017).

42. Legal scholars call this type of provision a "Henry VIII clause" in reference to the 1539 Statute of Proclamations, which gave King Henry VIII power to legislate by proclamation. The United Kingdom's Donoughmore Committee on the Powers of Ministers has said that this practice is "inconsistent with the principles of parliamentary government that the subordinate lawmaking authority should be given by the superior lawmaking authority power to amend a statute which has been passed by the superior authority." (Cited in Helen Xanthaki, *Thornton's Legislative Drafting*, 5th ed., Bloomsbury Professional, London, 2013, p. 420.) However, there are occasions where a Henry VIII clause is proper, such as when the delegated power is constrained and used only to ensure that the subordinate legislation continues to uphold the principles of the primary legislation. To read more about Henry VIII clauses, see Stephen Argument, *Henry VIII clauses: Fact sheet*, Standing Committee on Justice and Community Safety (performing the duties of a Scrutiny of Bills and Subordinate Legislation Committee), Legislative Assembly for the Australian Capital Territory, November 2011.

    While the existing jurisprudence suggests that such clauses are constitutional, it is noteworthy that the primary case cited – *In Re George Edwin Gray*, 57 SCR 150, 1918 CanLII 533 (SCC) – refers to Parliament's delegation of authorities to the Governor in Council under the 1914 *War Measures Act* to authorize:

    > acts and things and to make from time to time such orders and regulations as he may, by reason of the existence of real or apprehended war, deem necessary or advisable for the security, defence, peace, order and welfare of Canada.

43. *Crown Liability and Proceedings Act*, R.S.C. 1985, c. C-50.

44. *X (Re)*, 2016 FC 1105.

45. Ibid., paras. 255–257.

46. Federal government institutions, including the Canadian Security Intelligence Service (CSIS), must comply with the *Privacy Act*, which limits the disclosure of "information related to the physical or mental health of individuals." See Privacy Act, s. 77.

47. New section 11.16 empowers the minister to designate a person, including the director of CSIS or an employee, for the purposes of new section 11.17. However, at any given time, no more than one person is permitted to issue an authorization under new section 11.17.

48. As set out in new section 27.1(6), in accordance with regulations made under section 28 of the CSIS Act, all Federal Court hearings concerning section 27 matters are to be held in private.

49. *An Act to encourage and facilitate information sharing between Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada* (short title: *Security of Canada Information Sharing Act* [SCISA]), S.C. 2015, c. 20, s. 2.

50. *Anti-terrorism Act, 2015*.

51. SCISA, s. 3.

52. Schedule 3 of the SCISA lists the following organizations: Canada Border Services Agency; Canada Revenue Agency; Canadian Armed Forces; Canadian Food Inspection Agency; Canadian Nuclear Safety Commission; Canadian Security Intelligence Service; Communications Security Establishment; Department of Citizenship and Immigration; Department of Finance; Department of Foreign Affairs, Trade and Development; Department of Health; Department of National Defence; Department of Public Safety and Emergency Preparedness; Department of Transport; Financial Transactions and Reports Analysis Centre of Canada; Public Health Agency of Canada; and Royal Canadian Mounted Police.

53. SECU, *Minutes of Proceedings*, 1st Session, 42nd Parliament, 14 June 2016.

54. SECU (2017), recommendations 22–26, p. 41.

55. House of Commons, Standing Committee on Access to Information, Privacy and Ethics [ETHI], *Minutes of Proceedings*, 1st Session, 42nd Parliament, 18 October 2016.

56. ETHI, *Safeguarding Canada's National Security While Protecting Canadians' Privacy Rights: Review of the Security of Canada Information Sharing Act (SCISA)*, Fifth Report, 1st Session, 42nd Parliament, May 2017.

57. Government of Canada (2016).

58. Hill and Knowlton Strategies, *National Security Consultations: What We Learned Report*.

59. Ibid.

60. Professors Craig Forcese and Kent Roach suggested in a brief to ETHI that "not all protest and advocacy should be exempted from the new information-sharing regime. Violent protest or advocacy of a sufficient scale *can* be a national security issue justifying information sharing." See Craig Forcese and Kent Roach, *Brief to the House of Commons' Standing Committee on Access to Information, Privacy and Ethics: Analysis and Proposals on the* Security of Canada Information Sharing Act, 3 November 2016, p. 4.

61. See SECU (2017); ETHI (2017); and Office of the Privacy Commissioner of Canada, *Consultation on Canada's National Security Framework: Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety Canada*, 5 December 2016.

62. ETHI (2017), recommendation 10, p. 63.

63. ETHI (2017); and Office of the Privacy Commissioner of Canada (2016).

64. *Public Safety Act, 2002*, S.C. 2004, c. 15.

65. *Aeronautics Act*, R.S.C. 1985, c. A-2.

66. *Secure Air Travel Act*, S.C. 2015, c. 20, s. 11.

67. As defined in sections 2 and 83.01(1) of the *Criminal Code*. It should be noted that section 8(1)(b)(i) of the *Secure Air Travel Act* specifically lists certain terrorism offences, as opposed to all of the terrorism offences in the Code.

68. Government of Canada (2016); and SECU (2017).

69. This schedule contains 34 items, including the passenger's name, date of birth, citizenship, gender, the names of the travel agency and travel agent that made the person's travel arrangements, whether the person's ticket for the flight is a one-way ticket, the city or country in which the travel begins, the itinerary cities, the person's destination, the pre-selected seat assignment, the tag numbers for the person's baggage, the person's address, the address of the travel agency that made the travel arrangements and the manner in which the person's ticket was paid for.

70. *Aeronautics Act*, "Schedule."

71. *Privacy Act*, s. 77.

72. *X (Re)*, para. 50.

73. The minister may extend the 60-day period in exceptional circumstances (see *Secure Air Travel Act*, s. 15(2)).

74. SECU (2017), recommendation 36, p. 43.

75. *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9.

76. *Secure Air Travel Act*, s. 16.

77. A special advocate's role is to act on behalf of the named person in the security certificate proceedings. Since 2008, special advocates review the information against the person named in the security certificate and can challenge the ministers' claim that the secret evidence may not be disclosed to the person; the relevance, reliability and sufficiency of the secret evidence; and the weight to be given to it. The information is then imparted by way of summary to the subject of the security certificate in order to allow that person to be reasonably informed of the case against him or her. After the special advocate receives the secret evidence, he or she may not communicate with anyone about the proceeding, including with the person named in the certificate, without first obtaining the judge's authorization to do so.

78. SECU (2017), recommendation 33, p. 42.

79. Government of Canada (2016), p. 14.

80. Hill and Knowlton Strategies, *National Security Consultations: What We Learned Report*.

81. Ibid.

82. Ibid.

83. Ibid.

84. Ibid.

85. Ibid.

86. SECU (2017), recommendations 16–21, pp. 40–41.

87. *Anti-terrorism Act*, S.C. 2001, c. 41. Note that the list of entities referred to in section 83.05(1) of the *Criminal Code* is not the only applicable list; see the Office of the Superintendent of Financial Institutions, *Anti-terrorism Financing*.

88. *Criminal Code*, s. 83.01(1).

89. Currently, the Government of Canada maintains lists of terrorist entities under three sets of regulations: *Regulations Establishing a List of Entities* made under section 83.05(1) of the *Criminal Code*, *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*, and the *United Nations Al-Qaida and Taliban Regulations*. See Office of the Superintendent of Financial Institutions, *Anti-terrorism Financing*.

90. Public Safety Canada, *Listed Terrorist Entities*.

91. Simply being a member of a terrorist group is not in itself a criminal offence.

92. Public Safety Canada, *Listed Terrorist Entities*.

93. Ibid.

94. SECU, *Evidence*, 2nd Session, 41st Parliament, 10 March 2015, 0915 (Hon. Peter MacKay, Minister of Justice and Attorney General of Canada).

95. SECU (2017), p. 28.

96. Ibid.

97. *Application under s. 83.28 of the Criminal Code (Re)*, 2004 SCC 42; and *Vancouver Sun (Re)*, 2004 SCC 43.

98. *Youth Criminal Justice Act*, S.C. 2002, c. 1.

99. Ibid., ss. 3(1)(a)(i) and 3(1)(d)(i).

100. Laura Barnett et al., *Legislative Summary of Bill C-10: An Act to enact the Justice for Victims of Terrorism Act and to amend the State Immunity Act, the Criminal Code, the Controlled Drugs and Substances Act, the Corrections and Conditional Release Act, the Youth Criminal Justice Act, the Immigration and Refugee Protection Act and other Acts*, Publication no. 41-1-C10-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 17 February 2012.

101. *Canadian Passport Order*, SI/81-86. See, for example, section 10.1 of the Order.