Communications Security Establishment Commissioner

The Honourable Jean-Pierre Plouffe, CD

Commissaire du Centre de la sécurité des télécommunications

L'honorable Jean-Pierre Plouffe, CD

February 23, 2018

The Honourable John McKay, MP
Chair
Standing Committee on Public Safety and National Security
House of Commons
6th Floor, 131 Queen Street
Ottawa, Ontario K1A 0A6

Dear Mr. McKay:

On January 30th, 2018, I appeared as a witness before the Standing Committee on Public Safety and National Security with respect to Bill C-59, *An Act respecting national security matters*. On the same day, I tabled before the committee a covering letter to you along with additional proposals respecting Part 2 of the Bill, the *Intelligence Commissioner Act,* and Part 3, the *Communications Security Establishment Act* that had been provided to Ministers Goodale and Sajjan in November 2017.

As stated in my December 6, 2017 letter to you, I have continued my study and assessment of Bill C-59 as it affects the role of the Intelligence Commissioner (IC). As you know, given the quasi-judicial function of the IC, I am directly implicated in some of the proposed/amended Acts covered by the Bill.

Therefore, please find enclosed new additional proposed amendments with respect to Part 3, the *Communications Security Establishment Act* and Part 4, the *Canadian Security Intelligence Service Act.* The same package is also being sent to the two Ministers.

Le 23 février 2018

L'honorable John McKay, député
Président
Comité permanent de la sécurité publique et nationale
Chambre des communes
131, rue Queen, 6e étage
Ottawa (Ontario) K1A 0A6

Monsieur McKay,

Le 30 janvier 2018, j'ai comparu devant le Comité permanent de la sécurité publique et nationale à titre de témoin relativement au projet de loi C-59, *Loi concernant des questions de sécurité nationale*. Le jour même, j'ai déposé auprès du comité une lettre couverture ainsi que des propositions d'amendements supplémentaires concernant la partie 2 du projet de loi, la *Loi sur le commissaire au renseignement*, et la partie 3, la *Loi sur le Centre de la sécurité des télécommunications,* qui avaient été envoyées aux ministres Goodale et Sajjan au mois de novembre dernier.

Tel qu'indiqué dans une lettre datée du 6 décembre 2017 que je vous ai adressée, j'ai continué mon étude et évaluation des dispositions du projet de loi C-59 qui sont reliées à mon rôle de commissaire au renseignement. Comme vous le savez, compte tenu de la fonction quasi judiciaire du commissaire au renseignement, je suis directement touché par certaines lois proposées ou amendées par ledit projet de loi.

Dans ce contexte, veuillez trouver sous pli de nouvelles propositions d'amendements relativement à la partie 3, la *Loi sur le Centre de la sécurité des télécommunications*, ainsi qu'à la partie 4, la *Loi sur le Service canadien de renseignement de sécurité*. Ces propositions seront aussi envoyées aux deux ministres.

P.O. Box/C.P. 1474, Station "B" / Succursale «B»
Ottawa, Ontario K1P 5P6
Tel: 613-992-3044, Fax: 613-992-4096
info@ocsec-bccst.gc.ca

I am available to appear before the committee once again to discuss any of these matters and/or to address any issues that you may have or want to raise. Alternatively, I am prepared to communicate my views in writing, if you prefer.

Je demeure disponible afin de comparaître de nouveau devant le comité afin de discuter de tous ces sujets et/ou afin de répondre à toutes questions y afférentes que vous pourriez avoir. Si vous le préférez, je pourrais alternativement vous communiquer mes vues par écrit.

The Honourable/l'honorable Jean-Pierre Plouffe, CD

Additional Proposals of Amendments

Our continued study of Bill C-59 has lead us to identify additional proposed amendments. Some are more technical while a few are of a substantive nature.

CSIS Act

1. Amend the definition of dataset

The definition of dataset is very narrow, ie "means a collection of information stored as an electronic record and characterized by a common subject matter". Therefore, a dataset clearly has a connotation of an "already put together collection of information" (an entity) that forms and is "stored as an electronic record". Subsection 11.05(1) that governs the collection of a dataset is therefore relating to the collection of this entity and not of information that, put together with other information, would form an entity. We have been told by the government that the definition also covers both the collection of individual pieces of information and entities. We do not share that view and suggest an amendment be made to clarify the definition of dataset.

2. Amend paragraph 11.22(2) (c)

That paragraph currently states: "*The Director's authorization shall contain the following: (c) the grounds on which the Director concludes that the query would produce the intelligence referred to in subparagraph (1)(b)(i) or (ii)*". Subparagraph (ii) does refer to intelligence being acquired by the query, but subparagraph (i) refers to "to preserve the life or safety of any individual". We believe that the language of 11.22(2) (c) should reflect that and use language that would cover sub (i) as well. We would suggest replacing the language with: "…*would fulfill the purpose referred to in (1)(b)(i) and (ii)*."

3. Amend subsection 11.03(3), and sections 11.18 and 11.23

The language appearing in subsection 11.03(3) and in section 11.18 should also be reflected in section 11.23, by adding the notion of "notification of the determination for the purpose of the review and approval under the *Intelligence Commissioner Act"* to make it consistent. In addition, all three provisions should also make it clear that all the information that was before the Minister or the Director for decision-making purposes will be presented to the Intelligence Commissioner at the same time that the notification of the determination is made (to mirror subsection 23(1) of the *Intelligence Commissioner Act*).

4. Amend section 11.22 to provide for a period of validity of the exigent circumstances authorization

Section 11.22 does not provide for any period of validity of the exigent circumstances authorization to query. We believe that there should be one. The statute does provide that an application for the retention of that dataset must be made to the Federal Court. See

subsection 11.13(1) and paragraph 11.22(2) (f). In fact, the Service will need to make this application pursuant to section 11.13 as soon as feasible but no later than within 90 days after the day on which the dataset was collected and that it will have to be destroyed otherwise (see subsections 11.19(1) and (3)). But the period of validity for this urgent query should not be 90 days by default. It should be shorter. By comparison, section 43 of the *CSE Act* in Bill C-59 provides that emergency authorizations for foreign intelligence and cybersecurity may be valid for a period not exceeding 5 days.

5. Make consistent use of the word "personally" when referring to the Minister

Subsection 20.1(6) provides that "The Minister may personally…". The word "personally" is not used in either section 11.03 or subsection 11.04(1) when referring to the Minister issuing an authorization. At the same time, subsection 11.16(1) provides that the Minister may designate a person for the purpose of section 11.17. Given that there is no such wording as that of subsection 11.16(1) for sections 11.03 or 11.04, we must conclude that the decision should be made by the Minister personally. So the approach should be consistent either by using the word "personally" or not. That said, we note that section 48 of the *CSE Act* provides the Minister must personally exercise the powers set out in the legislation. This approach could be mirrored in the *CSIS Act* with the one exception.

6. Have sections 11.01 and ss apply "notwithstanding" the regime of section 2 and subsection 12(1) of the *CSIS Act.*

Our study of the datasets provisions has lead us to conclude that there may be an issue with respect to the lower legal threshold dealing with the collection and retention of datasets in sections 11.01 and ss. For instance, subsection 11.05(1) of the *CSIS Act* provides that the collection of datasets can occur if the Minister is satisfied that the dataset is relevant to the performance of CSIS duties and functions. Indeed, we believe that, as it currently reads in Bill C-59, the legal regime applying to section 12 of the *CSIS Act* will apply to all activities related to datasets, even if that was not the intent. Recent Federal Court decisions have made the following principles very clear:

- Subsection 12(1) (collection and retention of information) and section 2 (definition of threat related activity) of the *CSIS Act* form the core of CSIS essential function.
- CSIS can collect and retain, but only to the extent strictly necessary, threat related information, and it cannot collect any other type of information.
- Information falling outside of the scope of the definition of threat related information (eg datasets typically) cannot be collected but if it happens to have been collected, it cannot be retained unless it is strictly necessary to do so.
- These principles apply to all information collected by CSIS, including datasets.
- There is no provision in the proposed *CSIS Act* that (1) either amends the general principles found in subsection 12(1) and section 2 discussed above, or (2) that restricts their general application in any way when it comes to datasets.

Making sections 11.01 and ss apply notwithstanding any other provision in the *CSIS Act* may be a solution.

7. Amend the definition of "publicly available dataset" in subsection 11.01

The proposed definition simply refers the reader to paragraph 11.07(1) (a) by stating "means a dataset referred to in paragraph 11.17(1) (a)". That paragraph does not add or help in any way to understand the notion of publicly available as it says "was publicly available at the time of collection".

The rationale for having a meaningful definition is primarily due to the fact that publicly available datasets are not subject to any form of control, and therefore could, for instance, be retained for an indefinite period of time (in contrast, Canadian datasets can be ordered retained by the Federal Court for no more than two years- subsection 11.14(2) of the *CSIS Act* and foreign datasets may be authorized by the Minister to be retained for no more than five years – subsection 11.17(3) of the *CSIS Act*). Indeed, all non-public datasets will be divided into two categories in the Act of either Canadian datasets or foreign datasets (obviously the publicly available datasets category will also cover Canadian and foreign datasets as no other datasets are possible), which are both governed by sections 11.01 and ss. Having a meaningful definition for this very important concept will help the Service in evaluating datasets collected under s. 11.05 (s. 11.07).

8. Amend section 11.11 to clarify that the querying and exploitation of publicly available datasets should meet the requirement for the querying and exploitation of Canadian and foreign datasets pursuant to section 11.2

Section 11.2 states that once it has been authorized to be retained either by the Federal Court or the Minister, a Canadian dataset or a foreign dataset may be queried or exploited by a designated employee "to the extent that it is strictly necessary"… "to assist the Service in the performance of its duties and functions under sections 12 and 12.1" and "12, 12.1 and 15' in the case of foreign datasets. Section 11.11 uses language in its subsections (1) and (2) that relates to section 12, ie "for the purposes of section 12 to 16" and " in accordance with sections 12 to 16" respectively. However, the words "to the extent that it is strictly necessary" are not used and should be, given that they are used elsewhere in the same Act, ie in section 11.2. The rules of legislative interpretation could bring one to conclude that the absence of those words in that section is meaningful, was done purposely, and that it was Parliament's intention not to have them inserted and that they should not be "read in" as such.

9. Amend section 20.1 to ensure a broader scope of exemption for CSIS employees

We note that the justification for acts or omissions scheme found in section 20.1 of the CSIS Act is based on "information and intelligence collection activities". We see this reflected in subsections 20.1(6), (7), (8), (10) and in (11) where the test is applied. There could be a risk that the exemption scheme could be interpreted narrowly as being limited only to "collection activities" per se, ie specific activities aimed at collection as opposed to also covering a broader scope of activities that could be engaged in by employees in the context of the duties an functions falling under section 12 of the mandate. So it might be prudent to use language

like "engaged in activities for the Service in the performance of its duties and functions under section 12 of the CSIS Act."

This is especially true when considering the provision protecting CSE employees in section 50 of the CSE Act which is much clearer than what is found in the proposed amendments to CSIS Act. And the CSE provision specifically refers to both civil and criminal liability as being exempted. This underlines a disparity between the two systems.

CSE Act

10. Amend the provisions falling under the Procedure part of the *CSE Act* (sections 34 to 37) to ensure that the Intelligence Commissioner can review the full content of an authorization.

Subsection 34(2) of the *CSE Act* states that the Chief must establish that any authorization is necessary and that the conditions for issuing it have been met. The conditions are in subsections 35(1), (2), (3) and (4) depending on the type of authorization is being considered and are based on a reasonable grounds to believe test. Then section 36 deals with the content of an authorization, what it must specify. Subsection 36(d), (e) and (f) refer to terms, conditions and restrictions that the Minister may issue. However, these terms, conditions and restrictions are not part of the application process and are not contemplated in section 35 either. Therefore, it may be that no information will have been submitted to the Minister justifying why certain terms, conditions or restrictions should be issued, and the Intelligence Commissioner may not have any information to review and base his decision on. Apart from that, it is unclear whether the Commissioner could review those terms, conditions and restrictions on a reasonableness basis. Therefore, it would be important to amend subsection 34(2)) so that it reads: "The application must set out the facts that would allow the Minister to conclude that there are reasonable grounds to believe that the authorization is necessary, with or without terms, conditions and restrictions, and that the conditions for issuing it are met."

11. Amend subsections 27(1), 30(1) and 31(1) of the *CSE Act* to ensure that the Minister can issue authorizations that will be lawful "despite any other law, including that of any foreign state" as opposed to the current and more limiting wording of "despite any other Act of Parliament or of any foreign state". Proceed to amend subsections 28(1) and (2) of the same Act accordingly, save for the reference to foreign state.

The current *CSIS Act*, at its subsections 21(3.1) (collection and searches) and 21.1(4) (threat diminishing activities), clearly stipulates the following:

Activities outside Canada
(3.1) Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize activities outside Canada to enable the Service to investigate a threat to the security of Canada.

Measures taken outside Canada

(4) Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize the measures specified in it to be taken outside Canada.

When this provision was added to the *CSIS Act* (Bill C-44), discussions took place over whether any judgment/order issued by the Federal Court in favor of CSIS would cover any breaches to international law and/or the laws of a foreign state that employees may be making when engaging in certain activities abroad. The decision was made to provide that the Federal Court authorizations would apply without regard to any other law, including that of any foreign state. The notion of "law" was retained because it is a wider concept than that of an "Act". Actually, an Act is included in the law of a country. The scheme is aimed at protecting CSIS employees from any potential unlawful/illegal activity that they could engage in, even from an international law perspective.

The proposed *CSE Act* is making, in subsections 27(1) (FI collection), 30(1) (defensive cyber operations) and 31(1) (active cyber operations), all their ministerial authorization schemes applicable *"despite any other Act of Parliament or of any foreign state".* Arguably, this would not cover the notion of international law as a reference to the notion of "law" would in the subsections, instead of using "Act". We fail to see how the reference to "Acts" could empower CSE to violate international law. This would also apply to the violations of other sources of foreign law, such as constitutional law, or the common law to name two. International law binds Canada and there is a lot of international law applicable to Canada that is not covered in foreign "Acts". It is therefore recommended to use the following language "*despite any other law, including that of any foreign state*" in the *CSE Act*.

To make matters consistent, subsections 28(1) and (2), who are only focused on an exception for "*any other Act of Parliament*", could be amended and provide for "*despite any other law*" as the *CSIS Act* provision does.