# The Law Union of Ontario's Brief to the Standing Committee on Public Safety and National Security on Bill C-51

**The Working Group on National Security of the Law Union of Ontario**

*1. Security of Canada Information Sharing Act*

We strongly advise against proceeding further with the *Security of Canada Information Sharing Act* as contained in Bill C-51. The proposed Act is unnecessary, over-reaching, and counter-productive. If enacted, it will lead to serious encroachments on personal privacy and civil liberties in Canada.

Information sharing among the government institutions with national security responsibilities is a critical part of Canada's strategy against terrorism. But the national security agencies do not need Bill C-51 to continue sharing information - they already have ample legal authority to do so. The issues identified in this area to date have not been legislative but managerial in nature, relating to the operational problems of co-ordinating information exchange and activities, ensuring interoperability of databases, reconciling the sometimes inconsistent dictates of intelligence gathering and law enforcement, and refereeing the inevitable institutional rivalries and turf wars. Bill C-51 will not solve these operational problems and if anything will exacerbate them.

We note that there has been no suggestion that the recent murders of Warrant Officer Patrice Vincent in St-Jean-sur-Richlieu and Corporal Nathan Cirillo in Ottawa were in any way the result of a failure of institutional information sharing. In our view, Bill C-51 would not have prevented these tragic events.

What Bill C-51 is meant to do is to facilitate access by government institutions with national security responsibilities to information, including personal data, held by other government institutions. Section 5 of the Act gives other government institutions the authority to provide "relevant" information to a government institution listed in Schedule 3, either on request or proactively. "Relevant" in this context would mean information potentially of use or interest to these government institutions in accordance with their new expanded responsibilities to detect, identify, analyze, prevent, investigate or disrupt "activities that undermine the security of Canada."

The proposed *Security of Canada Information Sharing Act* contains virtually no limits or controls over the access to personal information by the Schedule 3 institutions. The Act does not require any showing that the information disclosed relates to any specific suspected "activity that undermines the security of Canada" or to any ongoing investigation; it merely has to be relevant to a Schedule 3 institution's responsibility to detect, identify, analyze, prevent, investigate or disrupt "activities that undermine the security of Canada." The definition of an "activity that undermines the security of Canada" encompasses far more than terrorist activities and terrorism offences and creates vast and ill-defined jurisdictions and responsibilities for the 17 Schedule 3 institutions in this area. Accordingly the universe of information that may be said to be relevant to the Schedule 3 responsibilities is similarly vast and ill-defined. The determination of what may be relevant information is not subject to any oversight or review and in fact may be made by government officials with no intelligence analysis background and disclosed on a "proactive" basis.

The Act may in fact be counter-productive, unleashing a tsunami of information unrelated to counter-terrorism, thereby distracting from the task at hand – counter-terrorism -, diverting limited resources, and exacerbating existing problems with co-ordination of efforts and institutional rivalries. Not all Information is reliable and more information is not necessarily better. Information requires careful analysis in the context of other information in order to determine its accuracy, meaning and value. Inaccurate or misleading information can have devastating effects if acted upon as the case of Maher Arar so sadly demonstrates.

In our view, the *Security of Canada Information Sharing Act* if enacted will seriously erode Canada's protection of personal information regime. The guiding principles in the Act do not incorporate or advert to generally accepted principles for the protection of personal information, such as limited collection, use, disclosure and retention. There is no requirement that the information provided was lawfully collected and no obligation to update or correct on either the part of the providing or receiving institution. There is no provision requiring the receiving institution to delete or retract information it has received that does not reasonably relate to an activity that undermines the security of Canada. The Act does not place any restrictions on the use or disclosure of information received. There are no limits on retention in the Act.

The Act does refer to the intelligence principle of respect for caveats about the use of information but then overrides the principle by allowing unlimited use and distribution within the Schedule 13 institutions (subsection 5(2)) or to any person for any purpose (section 6). There is nothing in the Act to prevent a receiving institution from providing the information to a foreign state or a private company.

We do not believe that the *Privacy Act* will offer a significant check on the Act's disclosure provisions. The interplay between the proposed Act and the *Privacy Act* is difficult to determine at this time, given the vague and broad wording of the proposed Act, the absence of enabling regulations governing the disclosure and retention of information, and the availability of exemptions from the *Privacy Act* disclosure requirements either by express statutory or regulatory language or by implication. In our view, it is highly doubtful whether the Office of the Privacy Commissioner can adequately review or oversee the extensive disclosures of personal information either from the outside government institutions or within the 17 Schedule 3 institutions. Indeed, the Privacy Commissioner in his March 6 letter to the Committee noted the legal and practical difficulties the Act would create for his Office and recommended that Bill C-51 be amended to establish an independent expert body as well as a separate Parliamentary body to review the activities of the 17 agencies in this area.

The Act clearly envisages government institutions entering into information-sharing arrangements in order to "share information regularly" (subsection 4(c)). In our view these arrangements have the potential to permit virtually unlimited access to personal information. Arrangements for information sharing can run the gamut from protocols for the handling of written requests for disclosure from Schedule 3 institutions to log-in access to databases by Schedule 3 institution personnel, with or without audit or access trails to wholesale transfer to databases to a Schedule 3 institution for data mining purposes.

We are particularly concerned that the Act as drafted will pave the way for wholesale access to biometric databases held by Passport Canada and Citizenship and Immigration Canada (CIC). We note that the government backgrounder to the Act specifically highlighted the possible advantages of access to CIC or Passport Canada information. One unstated use would be to match surveillance photographs or video stills against the enormous databases of photographs held by Passport Canada and CIC. The technology is already here. Passport Canada has already implemented the use of facial recognition software to scan its entire passport database of photographs to generate a facial recognition alphanumeric photo identifier for each photo. This led in one case to the detection of a duplicate false passport and the charging of a man in Montreal. The Calgary police reportedly have implemented a facial recognition system using their database of mug shots. The Office of the Privacy Commissioner of Canada has already adverted to the privacy concerns caused by the coupling of facial recognition software to body-worn camera recordings made by police officers.

The definition of "activity that undermines the security of Canada" in the Act is particularly troubling and encompasses an enormous range of activity that hitherto was not thought to come within anyone's notion of national security. The definition covers "any activity … if it undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada." "Undermines" is not a term of legal art. The Oxford English Dictionary defines "undermine" as meaning to "lessen the effectiveness, power, or ability of, especially gradually or insidiously" and so activities that may gradually lessen the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada would presumably meet the definition. The references to "sovereignty" and "territorial integrity" would cover Quebec souverainistes and Aboriginal land claims.

The definition of "activity that undermines the security of Canada" delineates the jurisdiction and responsibilities of the Schedule 3 institutions under Section 5 of the Act to detect, identify, analyze, prevent, investigate or disrupt such activities and in turn these jurisdiction and responsibilities determine what information may be of use or interest in carrying out these mandates. Accordingly, the Act casts a vast and indeterminate dragnet for information.

The list of specific types of activities said to that undermine the security of Canada offers no comfort. Activities that interfere with "the economic and financial stability of Canada" can cover anything from shorting the Canadian dollar or downgrading government bond ratings to transportation or other "vital industry" strikes to environmentalist protests against the Oil Sands, pipeline construction, and shipping in environmentally sensitive or important regions. "Changing or unduly influencing a government in Canada by … unlawful means" would cover activities from office sit-in demonstrations to protest government policy to unlawful election tactics such as the Robocall scandal. The ambit of "an activity that takes place in Canada and undermines the security of another state" is not constrained by the restriction "by force or unlawful means" and so may capture lawful activities taken in Canada against the interests of another state. It can, and likely will, include lawful activities directed towards replacing a dictatorship with a democracy.

The saving clause – "For greater certainty, [activity that undermines the security of Canada] does not include lawful advocacy, protest, dissent and artistic expression." – offers no protection against overreaching assertions of jurisdiction and information collecting responsibilities. "Lawful" excludes a wide range of civil protest and civil disobedience, including demonstrations without permits, contrary to by-laws or in violation of highway traffic rules or picketing on private property. The saving clause only limits what falls under an "activity that undermines the security of Canada" and hence the ambit of the Schedule 3 institutions' jurisdiction and responsibilities. It does not directly affect what is relevant information under Section 5 of the Act. Information concerning a lawful protest may be relevant in the eyes of a government institution to preventing an activity that undermines the security of Canada on the theory that today's demonstrator may become tomorrow's terrorist. The history of the security services in determining what is legitimate protest and dissent does not provide any assurance that this time will be different.

*2. Secure Air Travel Act*

We have proposed a number of amendments to the *Secure Air Travel Act* in Appendix A, the most important of which are proposed amendments to provide for the assistance of a special advocate in appeals to the Federal Court in a manner analogous to security certificate appeals under Division 9 of the *Immigration and Refugee Protection Act*. The special advocate's role would be to protect the interests of the appellant when information or other evidence is heard in the absence of the appellant pursuant to subsection 16(6) (a) of the Act. The special advocate system represents a compromise between the government's interest in protecting confidential information and informants and the appellant's right to a fair hearing and, while not perfect, at least affords an opportunity to challenge assertions of confidentiality and to test the relevance, reliability, and sufficiency of the secret evidence. Without it, in our view the section 16 appeals under the Act would have an appearance of manifest unfairness and may not conform to *Charter* standards set out in the Supreme Court of Canada cases dealing with the constitutional validity of the security certificate system.

Other proposed amendments include:

i) Removing the 60 day limitation period for appeals to the Minister. The 60 day limitation period runs from the time the person has "been denied transportation as a result of a direction made under section 9." The reason for the denial may not be immediately obvious to the person concerned as it is illegal under the Act to disclose that a person is on the "no fly" list: subsection 22(3). Thus the 60 day limitation period may unfairly deny a person an opportunity to challenge as of right being listed. It also is unnecessary. This is a status-based issue not dependent on the circumstances of the original denial. It is not a slip-and-fall on a patch of ice.

ii) Requiring the appeal judge to remove the person's name from the "no-fly" list if the court allows the appeal. The proposed subsection 16(5) only provides that the judge "may" do so.

iii) Placing the onus on the Minister at the appeal hearing to establish reasonable grounds for the decision under section 8(1) of the Act.

*3. Criminal Code*

a) *83.221 Advocating or promoting commission of terrorism offences*

In our view, this new offence is both unnecessary and counter-productive. The current range of terrorism offences in the Criminal Code cover a vast range of prohibited communications relating to terrorism, including recruiting, teaching a skill or expertise to, and instructing (directly or indirectly) a person for a terrorist group or to commit a terrorism offence as well as the general terrorism offence of participating or contributing, directly or indirectly, to an activity of a terrorist group. These offences are complete whether or not the communication was successful. The offences of counseling, attempting or conspiring to commit a terrorism offence capture other communications in preparation for a terrorism offence, even if it is not committed. In addition, communications in relation to terrorist activities or offences can provide reasonable grounds for obtaining a terrorism peace bond application under sections 83.3 or 810.01. Communications that manage to avoid these sanctions but still fall under the proposed 83.221 are in our view not worth the negative impact on freedom of expression and negative effects on counter-terrorism initiatives that 83.221 will cause.

The new section is counter-productive to the government's strategy of building trust and partnerships with Canada's diverse Muslim communities in order to prevent and counter radicalization and violent extremism. It is hard to have an open dialogue with the threat of criminal proceedings for statements that may be deemed to be advocating or promoting the commission of terrorism offences in general. The proposed offence also sends the wrong message about the nature of Canada's democracy: well-meaning statements made in good faith in defense of beleaguered Muslim communities in the world may run afoul of the new section while Islamophobia, misrepresentations about Islam, and fear mongering about Muslims are tolerated as part of the cost of freedom of expression.

The proposed offence is overly broad and vague and provides no real guidance on what speech is prohibited. The criminal intent for the offence is too low and based on a recklessness standard that will permit convictions on someone else's "objective" meaning of statements rather the speaker's purpose and intent.

The proposed offence was modelled on the "wilful promotion of hatred" section of the Criminal Code but omits the defences provided for that offence. Thus truth is not a defense to an 83.221 charge nor is good faith religious argument or discussion of a subject of public interest.

We have proposed amendments in Appendix A to provide for a more appropriate criminal intent and for statutory defence and to preclude conviction for counseling or attempting to commit an 83.221 offence to avoid making the offence even more broad and nebulous.

b) *83.222(7) "terrorist propaganda"*

Similarly the definition of "terrorism propaganda" should be amended to incorporate statutory defences to prevent political commentary, academic blogging, and legitimate advocacy being swept into the

catch-all definition of "terrorist propaganda." The proposed amendment set out in Appendix A is consistent with the definition of "hate propaganda" in subsection 320(8).

c) *83.3 Preventive Arrest*

This section of the Criminal Code has never been used according to the annual reports filed under section 83.31. Which raises the question: if something has never been tried, how do you know it doesn't work? There is no evidence to suggest that the changes proposed in Bill C-51 – lowering the threshold for preventive arrest and lengthening the potential detention period to 7 days – will make any difference whatsoever.

The terrorism provisions in the *Criminal Code* create a complex and unfamiliar statutory framework for police, prosecutors, judges and defence counsel alike. The preventive sections such as 83.3 are particularly problematic since the evidence may come from both intelligence and law enforcement sources. In our view the government would be better heeding the recommendation of the Major Inquiry to create a Director of Terrorism Prosecutions rather than continuing to tinker with anti-terrorism provisions in this way.

d) *810.011 Terrorism Peace Bond*

Changing the standard for entering into a recognizance from "will" to "may" unacceptably lowers the threshold for a judge to impose significant conditions on a person's liberty. The test in effect moves from a reasonable likelihood to a reasonable possibility of the commission of a terrorism offence. There is no evidence to show that the current standard for the making of a terrorism peace bond has proven to be a problem.

The use of the word "may" in 810.011 connotes that a mere possibility that a terrorism offence may be committed in the future will suffice. This change lowers an already low threshold for obtaining a recognizance order. Under the amendments, the judge need only be satisfied that the informant (typically a police officer) has reasonable grounds to fear that a person may commit a terrorism offence. The standard protections afforded an accused in a criminal trial do not apply. The proceedings are considered not to involve an "offence" strictly speaking. Rather, they are regarded as "preventive" in nature. Proof beyond a reasonable doubt is not required. A meaningful hearing will be hard to come by. Hearsay evidence is admissible to show the existence of reasonable grounds and may include redacted information from confidential informers and confidential sources that the defendant cannot possibly challenge. The defendant has no absolute right to appear in person: on motion by the prosecutor he can be required to appear by video instead. The evidence at the hearing is directed not towards proof of a fact which is capable of dispute but rather the existence of a reasonable belief that there is a possibility that the defendant may commit an unspecified terrorism offence at some point in the future.

An 810.011 order can have a very serious impact on the defendant's right to liberty and security of the person. An 810.011 order can land the defendant in jail. The order requires the defendant to enter into a recognizance with or without sureties. There is no statutory limitation on the amount of the recognizance or the number of sureties that the defendant must meet in order to be released. Failure or refusal to enter into the recognizance can result in committal to jail for up to 12 months.
Breach of the recognizance is a criminal offence punishable by up to 4 years in prison. A breach can encompass a violation of a condition attached by the judge to the recognizance or, more generally, a failure "to keep the peace and be of good behaviour." The latter encompasses being charged with any offence or infraction, whether criminal, federal, provincial or municipal, and whether pending, convicted or acquitted, and any other behaviour that a judge may characterize as amounting to a breach of the peace or constituting bad behaviour.

The section 810.011 conditions can also severely restrict liberty and security of the person affected. The section provides a shopping list of specific conditions that, if imposed, can seriously restrict liberty, including wearing an electronic monitoring device, being subject to a curfew or the equivalent of house arrest, and being ordered to remain within a specified geographic area and not to leave it without written permission. A judge can similarly impose conditions that impact on security of the person, including being required to provide bodily samples, either on demand or at regular intervals, for drug or alcohol testing. The conditions can be imposed for up to 12 months (5 years if previously convicted of a terrorism offence).

In our view there is no need for this amendment and its effect on liberty and security rights is clearly disproportionate to any putative benefits it may confer.

*4. Canadian Security Intelligence Service Act*

We strongly oppose the proposed amendments to give CSIS quasi-police powers to take measure to reduce threats to the security of Canada. This runs entirely contrary to the recommendations of the McDonald Commission to separate intelligence gathering and analysis from law enforcement. It also turns a blind eye to the shameful history of dirty tricks perpetrated in the late 1960s and 1970s by the RCMP security service all in the name of national security. The unlawful and criminal acts included arson (barn burning), burglary of offices to obtain or copy documents and information, illegal surveillance, including unlawful wiretaps and bugs and unauthorized mail interception and opening, "disruption" campaigns involving the production and distribution of false documents and the spreading of slanderous or scandalous news intended to cause dissension in targeted groups; widespread access to personal information held in government files, including income tax filings and Unemployment Insurance records; and Interference with personal lives of targeted individuals, including approaching employers to have them fire and circulating defamatory information about them. This is by no means an exhaustive list of the types of activities engaged in the name of security as the RCMP destroyed relevant files prior to the holding of the McDonald Commission. We will never know the full extent of the illegal activities engaged in by the RCMP and Security Services during this period.

Section 21.1 authorizes a judge to grant CSIS agents a dispensation in effect from the laws and constitution of Canada in order take these measures. We have serious doubts whether a judge's warrant under section 21.1 could act as a limit prescribed by law in order to override the fundamental rights and freedoms granted by the *Charter*. At a minimum the section is an affront to the rule of law.

We also seriously doubt whether judicial review will operate as an effective check and oversight on measures contrary to the law and the constitution. The proceedings are *ex parte* and subject to CSIS' honouring of its obligations of full, frank and fair disclosure of all the relevant facts. In a similar context there are at least two cases where the information provided by CSIS to justify a security certificate fell short of these standards when queried by a special advocate. In the more transparent law enforcement context, the cases are legion where information relied on to obtain a search warrant or wiretap *ex* parte has been subsequently shown to be incomplete, misleading or false. The situation is worse for 21.1 applications: there can be no *ex post facto* challenge or review of the application by an interested party and there is not even a provision for a report back to the issuing judge as to the measures taken pursuant to the warrant.

In our view, the decision being asked of the judge – to pass on the reasonably proportionality of the proposed measures – is not within the usual mandate of the judiciary. The traditional role of a judge is to act as an independent arbiter between two or more parties weighing evidence relating to a fact in issue in relation to legal standards and past precedents. Here the judge is asked to decide on what are essentially operational matters. In doing so, the judge must rely solely on CSIS's assessment of the nature and seriousness of the threat and on what CSIS says are the available other measures. The judge will have no background in this complex area and no case law for guidance. The judge can raise questions but judges are, as they should be, typically uncomfortable about being cast in a role that mixes adjudication with advocacy. Section 21.1 does not provide for a report back to the judge; without feedback it is impossible for a judge to calibrate his or her decision-making.

We think that section 21.1 will undermine the public's confidence in the judiciary and its intelligence services. In effect, a judge will be asked to lend the authority, reputation and dignity of the office to a flawed and open-ended process. To date, CSIS has managed to avoid the type of major scandals that have tarnished other foreign intelligence services, largely in our view because it has been excluded from engaging in policing activities. Enacting section 21.1 will change that when the inevitable scandals come to light.

We have proposed a series of amendments in an attempt to address some of the obvious deficiencies in Bill C-51. One is to focus measures on reducing terrorist threats rather than the much broader definition of "threats to the security of Canada." The second is to propose that CSIS cannot detain or forcibly confine an individual when taking measures. This is to ensure that secret arrests and detentions and "enhanced" interrogations do not take place under the guise of taking measures. The third is to propose a definition of "other Canadian law" consistent with the McDonald Commission to cover "dirty tricks", that is unlawful acts that do not amount to a criminal offence. Fourth we propose a system of Use of Measure reports similar to that used in section 25.1 of the *Criminal Code.* Finally we adopt the

submissions by the Special Advocates on Bill C-51 that section 21 and 21.1 be amended to permit the judge hearing the application to appoint counsel where necessary to protect the constitutional rights of persoms whose interests may be affected by the proposed warrant.

*5. Immigration and Refugee Protection Act*

The Law Union of Ontario adopts the submissions by the Special Advocates on Bill C-51 on the amendments to *IRPA* set out in Part 5 of the bill. Full and frank disclosure is essential for meaningful review of a security certificate. The current *in camera* system with participation by carefully selected special advocates sworn to secrecy strikes a reasonable balance between the interests of national security and protection of confidential human sources and the interests of the person named in the certificate and society's interest in having a fair hearing in accordance with the principles of fundamental justice.

*About the Law Union of Ontario*

The Law Union of Ontario is a coalition of over 200 progressive lawyers, law students and legal workers active in such areas of social justice as policing, security intelligence, civil liberties, human rights, access to the justice and the environment among others. The Law Union of Ontario has a long history of engaging national security issues, practices and legislation, dating back to our inception in 1974 including making submissions to the McDonald Commission in 1978, the Senate Committee examining the original CSIS bill in 1983, the House Special Committee reviewing the CSIS Act and the new *Security Offences Act* in 1990, the House Sub-Committee on Public Safety and National Security in 2005 and the House Standing Committee on Public Safety and National Security in 2013 on Bill S-7 to re-introduce preventative arrest and investigative hearings for terrorism offences.

APPENDIX A: PROPOSED AMENDMENTS

***Criminal Code***

1. Amend 83.221 (Advocating or promoting terrorism offences) as follows:

83.221 (1) Every person who, by communicating statements, ~~knowingly~~ wilfully 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.

Add:

Defences

83.221 (3) No person shall be convicted of an offence under subsection (1)

(a) if the person establishes that the statements communicated were true;

(b) if, in good faith, the person expressed or attempted to establish by an argument an opinion on a political or religious subject or an opinion based on a belief in a religious text;

(c) if the statements were relevant to any subject of public interest, the discussion of which was intended for the public benefit, and if on reasonable grounds the person believed them to be true; or

(d) if, in good faith, the person intended to point out, for the purpose of removal, matters producing or tending to produce feelings of hatred toward an identifiable group in Canada.

No Counselling or Attempt to Commit

83.221 (4) No person shall be convicted of counseling to commit an offence under subsection (1) pursuant to section 464 or of attempting to commit an offence under subsection (1) pursuant to section 463.

2. Amend 83.222 (7) as follows:

"terrorist propaganda" means any writing, sign, visible representation or audio recording ~~that advocates or promotes the commission of terrorism offences in general—other than an offence under subsection 83.221(1)—or~~ the communication of which would constitute an offence under 83.221 (1) or the offence of counseling ~~counsels~~ the commission of a terrorism offence—other than an offence under subsection 83.221(1).

***Canadian Security Intelligence Service Act***

1. Amend 12.1 of the *Canadian Security Intelligence Service Act* as follows:

   12.1 (1) If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada involving terrorist activity or the commission of a terrorism offence, the Director may approve that the Service ~~may~~ take measures, within or outside Canada, to reduce the threat.

   Add:
   12.1 (4) No measure shall be taken under 12.1 or 21.2 to intercept a communication or obtain any information, record, document or thing that could be intercepted or obtained pursuant to a warrant issued under section 21 of this Act.

   12.1 (5) The Director shall designate an employee of the Service with the responsibility for the control and management of any approved or authorized measures pursuant to section 12.1 or 21.1 and for filing any Use of Measure reports pursuant to 12.3.

   12.1 (6) In this Act,

   "Canadian law" means any federal, provincial or municipal law and includes the common law and the Quebec Civil Code.

   "terrorist activity" and "terrorism offence" have the same meaning as in section 2 of the *Criminal Code*.

2. Amend 12.2 of the *Canadian Security Intelligence Service Act* as follows:

   12.2 (1) In taking measures pursuant to section 12.1 or 21.1 ~~to reduce a threat to the security of Canada~~, the Service shall not
   (a) cause, intentionally or by criminal negligence, death or bodily harm to an individual;
   (b) wilfully attempt in any manner to obstruct, pervert or defeat the course of justice; ~~or~~
   (c) violate the sexual integrity of an individual, or
   (d) forcibly confine or detain an individual.

3. Add 12.3 of the *Canadian Security Intelligence Service Act* as follows:

   Use of Measures Report
   12.3 (1) As soon as is feasible after the taking of the measure, the Service employee designated pursuant to subsection 12.1(4) shall file a written Use of Measures report with the Director describing the measure taken, any property or other economic damage or personal injury caused by

or associated with the measure, and any property, information, record, document or thing obtained during the course of the operation and assessing the effectiveness of the measure, including whether the taking of the measure was reasonable and proportional in the circumstances, having regard to the nature of the threat and the results of the measure taken, and whether its execution contravened a right or freedom guaranteed by the Canadian Charter of Rights and Freedoms, was contrary to other Canadian law, or violated subsection 12.2 (1).

12.3 (2) Where the measure was authorized by warrant pursuant to section 21.1, the Director shall as soon as practicable give the judge authorizing the warrant and the Review Committee a copy of the Use of Measures report together with any other information necessary in the opinion of the Director to clarify, explain or amplify upon the information contained in the report.

4. Amend 21.1 (1) as follows:

21.1 (1) If the Director ~~or any employee who is designated by the Minister for the purpose~~ believes on reasonable grounds that a warrant under this section is required to enable the Service to take measures, within or outside Canada, to reduce a threat to the security of Canada, the Director or ~~employee~~ any employee who is designated by the Minister for the purpose may, after having obtained the Minister's approval, make an application in accordance with subsection (2) to a judge for a warrant under this section.

5. Amend 21.1 (2) as follows:

(2) An application to a judge under subsection (1) shall be made in writing and be accompanied by the applicant's affidavit deposing to the following matters:

(a) the facts relied on to justify the belief on reasonable grounds that a warrant under this section is required to enable the Service to take measures to reduce a threat to the security of Canada involving terrorist activity or the commission of a terrorism offence;

(b) the measures proposed to be taken;

(b.1) the nature of the threat;

(b.2) the Canadian laws or right or freedom guaranteed by the Canadian Charter of Rights and Freedoms that the measure will likely contravene or infringe;

(b.3) the likelihood that the measure will cause property or other economic damage or person injury;

(c) the reasonableness and proportionality, in the circumstances, of the proposed measures, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat, including whether other measures have been tried and have

failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to reduce the threat without resort to the proposed measure, or that without a warrant under this section it is likely that the threat to the security of Canada would not be reduced;

(d) the identity of the persons, if known, who are directly affected by the proposed measures and the nature of their involvement, if any, with the threat;

(e) the persons or classes of persons to whom the warrant is proposed to be directed;

(e) a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given;

(g) the period, not exceeding 60 days or 120 days, as the case may be, for which the warrant is requested to be in force that is applicable by virtue of subsection(6); and

(h) any previous application made under subsection (1) in relation to a person who is identified in the affidavit in accordance with paragraph (d), the date on which each such application was made, the name of the judge to whom it was made and the judge's decision on it.

6. Amend 22.1 (1) as follows:

22.1 (1) On application in writing to a judge for the renewal of a warrant issued under subsection 21.1(3) made by a person who is entitled, after having obtained the Minister's approval, to apply for such a warrant and who believes on reasonable grounds that the warrant continues to be required to enable the Service to take the measures specified in it to reduce a threat to the security of Canada involving terrorist activity or the commission of a terrorism offence, the judge may renew the warrant if the judge is satisfied by evidence on oath of the following matters:

(a) the facts relied on to justify the belief on reasonable grounds that the warrant continues to be required to enable the Service to take the measures specified in it to reduce a threat to the security of Canada involving terrorist activity or the commission of a terrorism offence; and

(b) the continued reasonableness and proportionality, in the circumstances, of the measures specified in the warrant, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat.

7. Amend 26 to remove the reference to 21.1:
26. Part VI of the Criminal Code does not apply in relation to any interception of a communication under the authority of a warrant issued under section 21 ~~or 21.1~~ or in relation to any communication so intercepted.

***Secure Air Travel Act***

1. Amend 15 (1):

   15. (1) A listed person who has been denied transportation as a result of a direction made under section 9 may~~, within 60 days after the day on which they are denied transportation,~~ apply in writing to the Minister to have their name removed from the list.

2. Delete 15 .(2)

3. Amend 16 (5):

   16 (5) If the judge finds that ~~a decision made under section 15 is unreasonable~~ the Minister has not established reasonable grounds for placing the appellant on the list pursuant to subsection 8(1), the judge ~~may~~ shall order that the appellant's name be removed from the list.

4. Amend 16 (6):

   (6) The following provisions apply to appeals under this section:
   (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;

   (b.1) the judge shall appoint a person from the list referred to in subsection 85(1) of the *Immigration and Refugee Protection Act* to act as a special advocate in the proceeding after hearing representations from the appellant and the Minister and after giving particular consideration and weight to the preferences of the appellant;

5. Add 16 (6.1), (6.2) and (6.3):

   (6.1) For the purposes of paragraph (6)(f), reliable and appropriate evidence does not include information that is believed on reasonable grounds to have been obtained as a result of the use of torture within the meaning of section 269.1 of the Criminal Code, or cruel, inhuman or degrading treatment or punishment within the meaning of the Convention Against Torture.

   (6.2) If the appellant requests that a particular person be appointed under paragraph (6)(b.1), the judge shall appoint that person unless the judge is satisfied that
   (a) the appointment would result in the proceeding being unreasonably delayed;
   (b) the appointment would place the person in a conflict of interest; or

(c) the person has knowledge of information or other evidence whose disclosure would be injurious to national security or endanger the safety of any person and, in the circumstances, there is a risk of inadvertent disclosure of that information or other evidence.

(6.3) For greater certainty, the judge's power to appoint a person to act as a special advocate in a proceeding includes the power to terminate the appointment and to appoint another person.

6. Add 16.1, 16.2, 16.3, 16.4 and 16.5:

16.1 (1) A special advocate's role is to protect the interests of the appellant in an appeal under section 16 when information or other evidence is heard in the absence of the public and of the appellant and their counsel.

(2) A special advocate may challenge

(a) the Minister's claim that the disclosure of information or other evidence would be injurious to national security or endanger the safety of any person; and

(b) the relevance, reliability and sufficiency of information or other evidence that is provided by the Minister and is not disclosed to the appellant and their counsel, and the weight to be given to it.

(3) For greater certainty, the special advocate is not a party to the proceeding and the relationship between the special advocate and the appellant is not that of solicitor and client.

(4) However, a communication between the appellant or their counsel and the special advocate that would be subject to solicitor-client privilege if the relationship were one of solicitor and client is deemed to be subject to solicitor-client privilege. For greater certainty, in respect of that communication, the special advocate is not a compellable witness in any proceeding.

16.2 A special advocate may

(a) make oral and written submissions with respect to the information and other evidence that is provided by the Minister and is not disclosed to the appellant and their counsel;

(b) participate in, and cross-examine witnesses who testify during, any part of the proceeding that is held in the absence of the public and of the appellant and their counsel; and

(c) exercise, with the judge's authorization, any other powers that are necessary to protect the interests of the appellant.

16.3 A special advocate is not personally liable for anything they do or omit to do in good faith under this Act.

16.4 (1) The Minister shall, within a period set by the judge, provide the special advocate with a copy of all information and other evidence that is provided to the judge but that is not disclosed to the appellant and their counsel.

(2) After that information or other evidence is received by the special advocate, the special advocate may, during the remainder of the proceeding, communicate with another person about the proceeding only with the judge's authorization and subject to any conditions that the judge considers appropriate.

(3) If the special advocate is authorized to communicate with a person, the judge may prohibit that person from communicating with anyone else about the proceeding during the remainder of the proceeding or may impose conditions with respect to such a communication during that period.

16.5 With the exception of communications authorized by a judge, no person shall

(a) disclose information or other evidence that is disclosed to them under section 16.4 and that is treated as confidential by the judge presiding at the proceeding; or

(b) communicate with another person about the content of any part of a proceeding under section 16 that is heard in the absence of the public and of the appellant and their counsel.