RESPONSE OF THE GOVERNMENT OF CANADA TO THE FINAL REPORT OF
THE STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY

SUBCOMMITTEE ON THE REVIEW OF THE *ANTI-TERRORISM ACT*

RIGHTS, LIMITS, SECURITY:
A COMPREHENSIVE REVIEW OF THE ANTI-TERRORISM ACT AND RELATED ISSUES

Government of Canada Gouvernement du Canada

Canada

RESPONSE OF THE GOVERNMENT OF CANADA

TO THE FINAL REPORT OF THE HOUSE OF COMMONS

STANDING COMMITTEE ON PUBLIC SAFETY

AND NATIONAL SECURITY

SUBCOMMITTEE ON THE REVIEW OF THE

ANTI-TERRORISM ACT

****

RIGHTS, LIMITS, SECURITY:

A COMPREHENSIVE REVIEW OF THE ANTI-TERRORISM ACT

AND RELATED ISSUES

TABLE OF CONTENTS

Response of the Government of Canada
to the Final Report of the House of Commons
Standing Committee on Public Safety and National Security
Subcommittee on the Review of the *Anti-terrorism Act*

****

Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues

INTRODUCTION

The Parliamentary Review of the *Anti-terrorism Act* (ATA) provided a useful opportunity to revisit the provisions that were enacted more than five years ago, as well as to examine other more current issues. For this reason, the Government of Canada has actively supported and participated in the reviews of the ATA conducted by committees of the House of Commons and the Senate pursuant to section 145 of the Act. The Government applauds the comprehensive effort undertaken by both committees and is grateful for the wealth and variety of witness testimony.

The Government is committed to ensuring that these laws continue to meet the needs of Canadians and that is why it has been very supportive of the Review. The laws must protect national security while respecting human rights, and they must provide a solid foundation that enables the Government to respond to the threat posed by terrorism in a concerted, effective and comprehensive manner.

As a precursor to a legislative response, the Government welcomes the opportunity to submit this written response to the recommendations made by the House of Commons Subcommittee on the Review of the *Anti-terrorism Act.*

A. THE *CRIMINAL CODE*: DEFINITIONAL ISSUES AND TERRORIST ACTIVITY OFFENCES (RECOMMENDATIONS 1 - 15)

1. The Criminal Code *definition of "terrorist activity"*

Defining terrorism in ways which clearly focus on the essence of the problem and distinguish it from other more conventional forms of crime, for the purposes of determining the application of criminal liability and investigative and preventive measures, represents a major challenge for the international community and for legislatures around the world. In its Report, the Subcommittee observed that the Canadian statutory definition of "terrorist activity" is complex and not easily understood. However, it also noted that this is not surprising, because "the phenomenon it attempts to define for criminal law purposes, terrorist activity in the early twenty-first century, is constantly changing in the forms and actions it takes." The Subcommittee considered other definitions proposed in briefs and submissions. In particular, it also reviewed the definition contained in the *International Convention for the Suppression of the Financing of Terrorism*,[1] and found that definition to be too narrow because it focused on activities involving only serious violence. It preferred the definition of "terrorist activity" adopted by Parliament in 2001.

The definition of "terrorist activity" in section 83.01 of the *Criminal Code* has two components. The first component incorporates a series of offences enacted to implement international legal instruments against terrorism. The second, more general, stand-alone component, states that a "terrorist activity" is an act or omission undertaken "in whole or in part for a political, religious, or ideological purpose, objective or cause" that is intended to intimidate the public or compel a person, government or organization to do or refrain from doing any act, if the act or omission intentionally causes a specified serious harm. Specified harms include causing death or serious bodily harm, endangering life, causing a serious risk to health or safety, causing substantial property damage where it would also cause one of the above listed harms and, in certain circumstances, causing

[1] A/RES/54/109, Annex, of 9 December 1999.

serious interference or disruption of an essential service, facility or system, whether public or private.

Some hold the view that the stand-alone definition is overbroad and that the reference to motive of political, religious or ideological purpose may invite "profiling" on the basis of politics, religion or ideology. This issue of the motive requirement is currently before the courts in *R.* v. *Khawaja*.[2] There are also some concerns that the elements which relate to seriously interfering with or disrupting an essential service might extend anti-terrorism measures to unlawful but peaceful labour strikes or other protests. These concerns were also raised in 2001 and, in response, Parliament included in the section an exception for advocacy, protest, dissent and stoppage of work, provided these activities are not intended to cause any of the other serious forms of harm referred to in the definition.

Recognizing the variety of views expressed on this important issue, the Government concurs with the Subcommittee recommendation. Within the existing formulation, the requirement that an act or omission must have been undertaken "in whole or in part for a political, religious, or ideological purpose, objective or cause" operates to narrow the scope of the definition, helping to distinguish terrorist activity from other, more conventional forms of criminal activity. It also provides an additional safeguard for an accused, since the prosecution must prove this motive beyond a reasonable doubt. Moreover, the Subcommittee's recommendation is consistent with recent independent reviews of the definition of terrorism in Australia and the United Kingdom, which concluded that similar motive requirements in their legislation should remain unchanged. The Government may reconsider the definition in light of judicial assessments once the litigation in *Khawaja* has concluded.

Non-legislative measures, such as training and review requirements, designed to ensure that criteria related to politics, race, religion or ideology are not used inappropriately, were also reviewed by the Subcommittee. These measures have been in place for some time and are always subject to review and improvement to ensure that Canada's law

[2] 2006 O.J. 4245, 2006-10-24

enforcement and security agencies perform their functions effectively while maintaining positive relationships with all communities. The Government of Canada believes that such positive relationships must be forged at the operational level and that non-legislative measures are, therefore, critical.

A number of concrete steps have been taken to develop a dialogue with Canada's diverse communities to foster understanding, trust, and cooperation between those communities and law enforcement, border and security agencies. These activities include grassroots community outreach initiatives, specific initiatives to address the concerns of Canada's Muslim and Arab communities, public liaison and regional outreach activities, and national initiatives to engage a dialogue on national security measures, such as the creation of the Cross-Cultural Roundtable on Security. Consisting of representatives from a cross-section of Canadian communities, the Roundtable is an important component of the Government's national security strategy. Its mandate is to engage Canadians and the Government in an ongoing dialogue on national security in our diverse and pluralistic society. Since its inception, it has provided valuable insights regarding the impact of security measures and has been engaged in a number of outreach activities across the country such as regional symposia bringing together members of ethno-cultural groups and government and national security officials to exchange views on matters related to national security.

It is also important to highlight some of the external and internal review mechanisms to which our law enforcement and security intelligence agencies are subject. These provide an avenue for the assessment of public complaints and for independent investigations into police, border and security intelligence conduct. The Security Intelligence Review Committee (SIRC) is an example of an independent civilian review body which reports to Parliament on the activities of the Canadian Security Intelligence Service (CSIS). Similar functions are performed by the Commissioner of the Communication Security Establishment (CSE). As well, Part II of the Report of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar recommended expanding the review of law enforcement's national security activities. The Government is considering

these recommendations and will advance a response in due course.

2. Other substantive issues

After considering the balance between the need for effective anti-terrorism provisions and freedom of expression, the Subcommittee also recommended the creation of a new offence of the glorification of terrorism for the purpose of emulation. The Government will carefully consider whether such an offence ought to be created, bearing in mind the *Canadian Charter of Rights and Freedoms* (*Charter*) and the policy implications.

With regard to subsection 83.22(1) of the *Criminal Code*, which provides that it is a crime to knowingly instruct any person to carry out a terrorist activity, the Government agrees with the recommendation that the provision should be expanded to include an instruction to a person to facilitate the carrying out of a terrorist activity.[3] However, the Government does not believe that the same change is needed in subsection 83.21(1), which provides that it is a crime to knowingly instruct any person to carry out any activity for the benefit of a terrorist group, because the present formulation is already broad enough to include instruction to facilitate the carrying out of such activity.

Representatives of the legal profession have expressed the view that the offence of knowingly contributing to the ability of a terrorist group to facilitate or carry out a terrorist activity, in section 83.18 of the *Criminal Code*, might extend to legal counsel providing legal services to those accused of terrorism offences. The Subcommittee recommended amendments to ensure that legal counsel could function without fear of prosecution. The Government believes that the existing *mens rea* (*i.e.* mental element) requirements and other safeguards, including the application of *Charter* rights to legal representation, are sufficient. The Government believes that the solicitor-client privilege should not be used as a shield to conceal *knowing* participation in or *knowing* contribution to a terrorist group.

---

[3] Where the Government agrees with or supports, or accepts a recommendation, further and separate Cabinet consideration would, nevertheless, be required to implement such a recommendation.

The Subcommittee recommended limiting the discretion of the Attorney General of Canada to commence a terrorism prosecution anywhere in Canada. Notwithstanding this recommendation, the national security and evidentiary aspects of a major terrorism case, as well as the complexity and logistical challenges raised, may require the use of special facilities which are not available in every part of Canada. It may be essential to the interests of justice or the security of Canadians, as well as the interests of the accused, that proceedings be conducted in appropriate locations and facilities. Moreover, advances in transportation, information and communications technologies have made the transfer of cases far less prejudicial than would have been the case in previous decades. The Government believes that a trial should be held where there are appropriate facilities which are essential in such cases.

The Subcommittee also recommended that the offence of harbouring or concealing, in section 83.23 of the *Criminal Code*, be expanded. The offence was designed to specifically address the situation where someone *knowingly* harbours or conceals another person who he or she *knows* has carried out a terrorist activity or is likely to carry out a terrorist activity and does so *for the purpose of enabling the person to facilitate or carry out a terrorist activity*. The focus of the offence is on harbouring or concealing a person to enable that person to facilitate or carry out a terrorist activity. In contrast, helping someone to escape after the commission of a terrorist activity would be caught by the accessory after the fact provisions in section 23 of the *Criminal Code*. The Subcommittee recommended maintaining the purpose requirement in respect of harbouring or concealing a person who is likely to carry out a terrorist activity, but creating a new crime of harbouring or concealing someone who has carried out a terrorist activity in the past, but without the added purpose requirement. This formulation would be broader than the existing accessory after the fact provisions, which include a purpose requirement, namely, to provide assistance for the purpose of enabling that person to escape. The Government believes that it would be preferable to continue the focus of section 83.23 on deterring conduct relating to future terrorist activity that might otherwise be facilitated or carried out. Given the comments of the Subcommittee, however, the Government will re-examine the wording of this offence and the applicable sentencing provisions. The

Subcommittee made a comparable recommendation[4] with respect to the similar harbouring and concealing offence in section 21 of the *Security of Information Act* and, generally speaking, the same reasoning and conclusions would apply.

Concerning punishments for multiple offences, the Subcommittee proposed to subject anyone who is convicted of knowingly participating in a terrorist activity to a maximum of life imprisonment. The Government believes that this is already addressed by sections 21 and 22 of the *Criminal Code*, by which anyone who aids or abets a crime, or who counsels someone else to commit a crime, is a party to the crime, and hence liable to the same punishment as the person who actually commits it. If the indictable offence constitutes a terrorist activity, section 83.27 generally substitutes life for the otherwise-applicable maximum sentence. As to the application of these sentences, the principle set out in section 83.26 of the *Criminal Code* is that consecutive sentences must be served in cases where there are multiple convictions for offences arising out of the same events or series of events and one of the convictions is in relation to a terrorism offence.

The Subcommittee also proposed that this principle be clarified in cases where a sentence is imposed for an indictable offence committed for the benefit of a terrorist group (section 83.2) so that in addition to the sentence imposed under section 83.2, a person can also be sentenced for the underlying indictable offence. However, the effect of section 83.2 is to create a crime that imposes a maximum punishment of life imprisonment in place of the otherwise-applicable punishment for the indictable offence, if that offence is committed for the benefit of a terrorist group. Thus, for example, fraud (section 380), which normally punishable by a maximum of 14 years, would become punishable by a maximum of life imprisonment under section 83.2 if the fraud were committed to finance a terrorist group. Section 83.26 provides that sentences imposed for certain terrorism offences, other than a sentence of life imprisonment, would have to be served consecutively to any other sentence arising out of the same event or series of events or to any other sentence to which the person is already subject.

[4] Recommendation 50.

B. THE *CRIMINAL CODE*: TERRORIST FINANCING AND TERRORISM-RELATED PROPERTY (RECOMMENDATIONS 16 - 22)

The ATA amended the *Criminal Code* to create criminal offences and imposed other requirements related to the financing of terrorism, implementing international obligations under Resolution 1373 of the UN Security Council and the *International Convention for the Suppression of the Financing of Terrorism.*

Section 83.1 of the *Criminal Code* requires everyone in Canada and Canadians anywhere to disclose to the Commissioner of the Royal Canadian Mounted Police (RCMP) and the Director of the Canadian Security Intelligence Service (CSIS) the existence of property in their control or possession that they know is owned or controlled by or on behalf of a terrorist group as well as any information about transactions or proposed transactions related to that property. Representatives of the legal profession have compared the section 83.1 requirement with anti money-laundering standards and have expressed concern that it could in some circumstances be inconsistent with solicitor-client privilege. The Subcommittee recommended that an amendment be made to exempt lawyers providing legal services. Long-established international standards against money-laundering require the reporting of suspicious transactions and elements of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) which implement those standards are based on reasonable grounds to suspect. The purpose of section 83.1 of the *Criminal Code*, on the other hand, in combination with section 83.08, is to freeze terrorism-related property and support seizure, and later forfeiture, measures. It requires reporting only where the subject actually knows that the property involved is owned or controlled by or on behalf of a terrorist group. In the area of terrorism, strong measures are needed to ensure Canadian conformity with international legal obligations and, as a matter of policy, the Government does not believe that the solicitor-client privilege should be used to conceal property or transactions if the solicitor has knowledge that they relate to terrorism. Therefore, the Government does not propose to make the recommended change.

Section 83.08 of the *Criminal Code* deals with freezing of terrorism-related property. Section 83.12 makes it an offence to knowingly deal in such property, engage in or facilitate transactions in respect of such property, or provide services in respect of such property for the benefit of or at the direction of a terrorist group. The Subcommittee recommended that a due diligence defence should be provided for this offence. While a due diligence defence applies in respect of strict liability offences, this is a criminal offence. In this case, the *mens rea* of knowledge is required. This is because for criminal offences, a subjective fault element is generally required. Thus, to establish that the accused "knowingly" dealt in terrorism-related property, for example, it would have to be proved beyond a reasonable doubt that he or she actually knew that the property was owned or controlled by a terrorist group.

The Subcommittee has also recommended that the words "wilfully and" be deleted from section 83.02 of the *Criminal Code*. However, the Government proposes to keep the present wording that is consistent with the wording found in the *International Convention for the Suppression of the Financing of Terrorism* and in UN Security Council Resolution 1373.

C. THE *UNITED NATIONS ACT* AND THE *CRIMINAL CODE*: LISTING OF TERRORIST ENTITIES (RECOMMENDATIONS 23 - 26)

Preventing terrorists from using the global financial system to further terrorist activity is essential for the suppression of international terrorism. A key element of the response of the international community has been to impose measures to prevent the concealment and transfer of funds or assets used to finance terrorism, and to designate individuals and other entities to whom these measures are to be applied by placing them on lists.

As a Member State of the United Nations and State Party to the *United Nations Charter*, Canada is legally obliged to give effect to measures imposed by binding resolutions of the Security Council; including the measures required by Resolution 1267, its successor resolutions and Resolution 1373. Canada has responded by establishing a process for the

listing of terrorist entities in order to apply specified measures, such as the freezing of assets, to those who are listed. This process has taken the form of three distinct, yet complementary terrorist listing mechanisms.

The first mechanism, the *United Nations Al-Qaida and Taliban Regulations* (UNAQTR) were made in 1999 under the *United Nations Act* to freeze the assets of entities belonging to or associated with the Taliban and Al-Qaida. These entities have been listed by the Committee of the UN Security Council mandated to enforce Resolution 1267 and its successor resolutions, and the list is updated by that committee from time to time.

The second mechanism, also made under the *United Nations Act*, consists of the more general *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* (RIUNRST), which create a Canadian list of terrorist entities not restricted in geographic and affiliative scope as is the UNAQTR. These implement more general requirements to suppress the financing of terrorism pursuant to Resolution 1373, which was adopted shortly after the attacks on the United States on September 11, 2001. This involves the application of measures mandated by the Security Council but, in the absence of an international consensus as to the identification or designation of the entities involved, the Council has left the decision as to which entities should be listed to Member States.

The third mechanism, established under the *Criminal Code*, enables the Government of Canada to apply appropriate criminal measures to entities, including those not necessarily listed by the first two mechanisms.

Taken together, the three mechanisms advance domestic security interests and support Canadian conformity with a range of international obligations, including those under Resolutions 1267 and its successors, Resolution 1373, as well as the International Convention for the *Suppression of the Financing of Terrorism* which the ATA enabled Canada to ratify.

The Subcommittee recommended that the Government consider further integration of the three listing mechanisms. In this regard, it should be noted that the Minister of Foreign Affairs is the responsible minister under the *United Nations Act* and as such is accountable to ensure that obligations imposed by Security Council resolutions on Canada are effectively implemented in Canada including through recommending listings under the *RIUNRST.* For his part, the Minister of Public Safety is responsible for law enforcement and intelligence activities and, therefore, is accountable for recommending listings under the *Criminal Code.* Accordingly, the Government is organized to support and deliver on these complementary ministerial accountabilities through Foreign Affairs and International Trade Canada, and Public Safety Canada.

It should be noted that Cabinet is collectively responsible, given that under both the *Criminal Code* and *RIUNRST,* the decision to list or de-list rests with the Governor in Council based on the recommendation of the accountable Ministers. Governmental process ensures that the full interdepartmental coordination takes place to allow for informed Cabinet decision-making.

The relationship between the law of Canada and applicable international legal instruments means that the mechanisms for listing and de-listing, as well as the consequences of listing, are different in each case.

The list of terrorist entities incorporated through the UNAQTR was created and is maintained by the UN, specifically the Al-Qaida and Taliban Sanctions Committee. Entities on this list are automatically incorporated into Canada's UNAQTR. The RIUNRST allows Canada to meet its obligations under UN Resolution 1373 to freeze "without delay" the funds and other financial assets of terrorist entities under the RIUNRST that have been listed by Canada, not by the United Nations. For these two lists, the consequences of listing are limited to those required by the Security Council and consist primarily of the freezing of assets and a prohibition on fundraising.

The third listing mechanism in the *Criminal Code* is established exclusively in Canadian law but nonetheless is an important element of Canada's implementation of the

International Convention for the Suppression of the Financing of Terrorism and Resolution 1373. This mechanism contains additional measures beyond those which implement the Security Council Resolutions. Any individual or entity listed becomes a "terrorist group", thereby triggering the potential laying of charges and prosecution under many of the *Criminal Code* terrorism offences, and some non-criminal measures such as the de-registration of a charity or the refusal to register an organization as a charity. In addition, there are provisions for the seizure and forfeiture of terrorist property.

As a result, the *Criminal Code* listing regime carries a higher standard, that is, the belief that the subject has *knowingly* been involved in a terrorist activity or acted on behalf of a terrorist entity. In contrast, the standard for the RIUNRST mechanism is based on the requirements of Resolution 1373.

Therefore, while a fully integrated listing regime would, on its face, appear to be desirable, the considerations set out above illustrate that these three mechanisms are aligned to an appropriate degree and offer complementary tools to counter terrorism and the financing of terrorism. In dealing with the same considerations of domestic and international law, other countries with legal systems similar to Canada's, such as Australia, the United States and the United Kingdom, have also established and maintained separate listing regimes.

With respect to the House Subcommittee's recommendation that more direct access to the courts be provided to challenge listing decisions, the Government would note that the role of Ministers is essential to ensure that decisions can be made as quickly as possible based on accurate and current security intelligence information. As such, enabling an entity to make a direct application for judicial review under the *Criminal Code* regime without first applying to the Minister of Public Safety would run counter to the goal of effective and timely decision-making. Furthermore, instituting a mechanism that automatically de-listed individuals or entities after a set period of time – either within the context of a request or as part of the two-year review of the *Criminal Code* list - could result in Canada failing to comply fully with its international obligations. Given the significant

implications this could carry for Canada's domestic security and international obligations, it is important that the current processes be maintained.

D. THE *CHARITIES REGISTRATION (SECURITY INFORMATION) ACT* AND THE *INCOME TAX ACT*: REFUSAL TO REGISTER AND DE-REGISTRATION OF CHARITIES (RECOMMENDATIONS 27 - 34)

Charities are a vital component of Canadian society. They help the sick and the disadvantaged, they promote education and provide community facilities and they provide humanitarian assistance throughout the world. Accordingly, Canadian charities registered under the *Income Tax Act* (ITA) benefit from a number of tax privileges. Chief among these are exemption from tax under Part 1 of the ITA and the ability to issue tax receipts that allow donors to claim a corresponding tax credit or tax deduction. However, domestic law enforcement and intelligence agencies, as well as international organizations such as the UN Security Council and the Financial Action Task Force, have all documented the direct or indirect financing of terrorism through organizations that also have or claim to have charitable goals. In response, Parliament enacted the *Charities Registration (Security Information) Act* (CRSIA) as part of the ATA. The CRSIA allows the Government to make use of classified information in deciding whether an organization should be registered or continue to be registered as a charity under the ITA.

The Minister of Public Safety and the Minister of National Revenue may, after consideration of classified information, sign a certificate stating that it is their opinion that there are reasonable grounds to believe that an applicant or a registered charity has made, makes or will make resources available, directly or indirectly, to an entity that engages or will engage in any terrorist activity as defined in the *Criminal Code*. Once a certificate is issued, it is automatically submitted to the Federal Court for judicial review. Once a judge of the Federal Court, after hearing all of the evidence, determines that a certificate is reasonable, the certificate becomes conclusive proof that an organization is ineligible to become or remain a registered charity. Under the CRSIA, a charity can apply to have Ministers review their decision to issue a certificate on the basis of a

material change in circumstances that led to the certificate action.

Taking into consideration the consequences of a decision to de-register or to refuse to register a charity, the Subcommittee recommended that such an outcome be precluded if it is established that the charity has exercised "due diligence" to avoid improper use of its resources and to limit refusal or de-registration to cases where the charity "knew or ought to have known" of the impropriety.

It should be understood that the process under the CRSIA is administrative. The CRSIA provides for an administrative measure (*i.e.* issuance of a certificate to permit the use and protection of classified information) resulting in an administrative remedy: revoking or refusing charitable registration, with the consequent lack of access to tax benefits. In addition, this approach is consistent with the ITA requirement that registered charities must control and remain accountable for the use of their resources. This requirement is lifted only when charities give their resources to a qualified recipient under the ITA.

Also, to maintain public confidence in the system of tax assistance for registered charities and to provide assurance to donors that charitable funds will be used exclusively for specified charitable purposes, the Government should make every effort to ensure that no benefit is extended to organizations that are linked to terrorism. To require in the CRSIA that an organization "knew or ought to have known" could, in some circumstances, effectively result in the Government of Canada providing a tax subsidy for resources tied to terrorism.

Further, incorporating a statutory defence of due diligence in conjunction with the establishment of detailed guidelines and a "checklist" to assess due diligence would make it possible for organizations with links to terrorism to use due diligence consultations to gain information about Canada's counter-terrorism measures and to structure their affairs so as to create a defence against the CRSIA regime.

The foregoing changes could also weaken Canada's conformity with the *International Convention for the Suppression of the Financing of Terrorism* and the Recommendations of the Financial Action Task Force.

Concerning judicial appeals under the CRSIA, the Government believes that further study is needed to assess the implications of recent judicial consideration of the provision governing access to appeals in the IRPA security certificate regime. There are also concerns that adding to the CRSIA a general prohibition on the publication of the identity of an organization, beginning from the time of investigation, and a general confidentiality ban on documents filed with the Federal Court, would depart from the principle of openness in court proceedings and would run a serious risk of contravening the *Charter*.

The Subcommittee has recommended that the words "at that time, and continue to be," be removed from paragraph 4(1)(b) of the CRSIA so that Ministers are not precluded from taking action to refuse or revoke a charity's registration if the terrorist organization to which it has provided resources ceases its terrorist activity before the Ministers have become aware of the assistance or are able to sign a certificate. This was not the result intended by this provision and the Government can, therefore, support the proposed amendment.

E. THE *CANADA EVIDENCE ACT* (RECOMMENDATIONS 35 - 43)

The ATA amended sections 37 and 38 of the *Canada Evidence Act* (CEA) to address the judicial balancing of interests when the disclosure of information in proceedings would encroach on a specified public interest and, in particular, would be injurious to international relations, national defence or national security. The reforms were designed to accomplish several objectives. They introduce greater flexibility into the system and offer the opportunity to resolve evidentiary issues early on in the proceedings. They also allow for use of information relating to international relations, national defence and national security in proceedings in a manner that is consistent with the right of an accused to a fair hearing, while at the same time preserving the federal government's ability to protect information, the disclosure of which would be injurious to these interests.

The purpose of the Attorney General certificate is to provide, where necessary, a bar to the disclosure of information in connection with a legal proceeding. A certificate may be

issued either to protect information that has been obtained in confidence from or in relation to a foreign entity, or to protect national defence or national security. Such information is often provided on the express condition that it not be disclosed. Canada is only in a position to provide the necessary guarantees to another state that information will not be disclosed if the ultimate decision is vested in the Attorney General of Canada and not the courts. In recent litigation concerning section 38 of the CEA, the federal Crown made the following argument: [5]

The consequences of a breach of the third party rule would be significant to Canada, given that it is generally a net importer of sensitive information. While other states may still be willing to share information with Canada, their calculations of risk and benefit might well be different in many cases if they considered as potentially unreliable Canada's ability to guarantee the protection of information that was given to it in confidence. This would, in turn, impair Canada's ability to combat terrorism.

The Attorney General also has the power to issue a *fiat* to take over and conduct any prosecution where sensitive or potentially injurious information is involved.

The Government believes that the current fifteen-year lifespan of an Attorney General certificate is not excessive, given the nature of the information at issue. However, the Government is prepared to accept the Subcommittee's recommendation that a certificate should expire after ten years, unless it is re-issued by the Attorney General of Canada pursuant to section 38.13(9). Many safeguards already apply to any use of the Attorney General certificate. For example, the certificate, and any variance or cancellation of the certificate, must be published without delay in the *Canada Gazette*. However, in the interests of enhancing transparency, the Government accepts the Subcommittee's recommendation that the CEA be amended to require the Attorney General of Canada to table an annual report in Parliament setting out the usage of the section 38.13 certificates and section 38.15 *fiats*. It is worth noting that although neither section has been invoked to date, both remain essential tools.

---

[5] *The Attorney General of Canada* v. *Mohammad Momin Khawaja*, Federal Court file number DES-2-06, Memorandum of Fact and Law of the Applicant (Constitutional Question), paragraph 21.

Currently, every party to a proceeding may apply to the Federal Court of Appeal for an order varying or cancelling the section 38.13 certificate and the judge who reviews the certificate may confirm, vary or cancel the certificate. The Government considers the existing judicial review mechanism to be adequate.

One of the new features introduced to section 38 of the CEA by the ATA was the requirement of certain persons to give notice to the Attorney General of Canada in circumstances where they expect to disclose or cause the disclosure of sensitive or potentially-injurious information. However, in respect of certain functions they perform, some entities (including Federal Court judges, the Information and Privacy Commissioners, and certain Commissions of Inquiry) were listed on the schedule to the CEA and, pursuant to paragraph 38.01(6)(d), are relieved of the need to give notice, except when they make a decision or order that would result in the release of such information.

These entities were added to the schedule because they have processes in place to protect sensitive information and potentially injurious information. As a result, the Government is not convinced that such entities are in need of written guidelines or need to establish review mechanisms to assist them in fulfilling their duty to prevent the disclosure of sensitive or potentially injurious information and to notify the Attorney General of Canada under subsection 38.02(1.1) of the CEA. Such guidelines might also be inappropriate in certain cases, such as in circumstances where judicial independence issues may be raised. That said, however, the Government would be pleased to respond to any requests to provide guidance on a case-by-case basis to the designated entities.

Following the giving of notice, under certain circumstances, applications may be made to the Federal Court under section 38.04 of the CEA. At present, the Attorney General of Canada bears the responsibility under the CEA of applying to the Federal Court on behalf of a witness who gives notice and the Subcommittee recommended that the Government bear the cost of the application. In such cases, the witness may be implicated in the

proceeding, but would likely not have commenced it, and, as a matter of policy, should not have to bear the financial burden of commencing an application before the Federal Court. In the case of other persons, including those who seek the disclosure of the information, however, the Government believes that they should continue to bear the burden of commencing an application, notwithstanding the recommendation of the Subcommittee to require the Attorney General to apply to the Federal Court for an order with respect to disclosure of the information in every case where, except by agreement with the party, the Attorney General does not permit full disclosure without conditions.

Having received notice, the Attorney General may be in a position to consent to the disclosure of such information. The person seeking disclosure has the right to make an application to the Federal Court ten days after having given notice if disclosure has been denied, in whole or in part, or if the Attorney General has not responded within the ten-day limit. Ten days is frequently not much time for the Attorney General to complete a review of the documentation, given the volumes of material that may be involved, as well as the necessity for internal consultations. If the person were willing to wait a little longer before making an application, there would be a greater opportunity of exploring the possibility of entering into a disclosure agreement with the Attorney General. Moreover, the Attorney General must also weigh the public interest in disclosure as well as the public interest in non-disclosure before pronouncing upon the issue. Consideration should also be given to the resource implications for the Federal Court if this change were to be made. For these reasons, the Government is not considering any alterations to the *status quo*.

Concerning the recommendation of the Subcommittee that section 37.21 of the CEA, which was repealed in 2004, be re-enacted, the Government notes that, in *Toronto Star Newspapers et al. v. R.*, the Federal Court held, *inter alia*, that subsection 38.11(1) of the CEA, which is the equivalent of section 37.21, violated the principle of judicial openness protected under paragraph 2(b) of the *Charter*. The Court took the remedial action of reading down the section so that it only applies to the *ex parte* requirements of the section 38 CEA regime. The Government did not appeal the decision.

The Supreme Court of Canada has also shown a strong support for the open court principle, even in light of national security considerations, in such cases as *Ruby* v. *Canada (Solicitor General)*[6] and *Reference re s. 83.28 of the Criminal Code*[7], dealing with the investigative hearing provision of the ATA. As a result, the Government does not share the view of the Subcommittee that the former section 37.21 of the CEA should be re-enacted. Section 37.21 was repealed in 2004 as a corrective measure.

Finally, the Government appreciates the recommendations from the Subcommittee concerning the need to improve the wording of subsection 37(7) of the CEA and to enact a provision akin to that subsection with respect to disclosure orders made under section 38.06. The Government agrees, in principle, with these recommendations.

F. THE *NATIONAL DEFENCE ACT*: COMMUNICATIONS SECURITY ESTABLISHMENT AND THE CSE COMMISSIONER (RECOMMENDATIONS 44 - 47)

The Government agrees that all of the activities of the Communications Security Establishment (CSE) must adhere strictly to the provisions of the *Charter* and the *Privacy Act*, in addition to all other laws of Canada. Indeed, operating scrupulously within the laws of Canada is the first pillar of the CSE's values and ethics code and it has implemented stringent measures to protect the privacy of Canadians. In particular, CSE takes very seriously its obligations under the *National Defence Act* (NDA), which prohibits CSE from directing its activities at Canadians, wherever they may be located, or anyone in Canada. Furthermore, the NDA mandates the CSE Commissioner to review CSE's activities to ensure they are lawful. As such, the Government believes that the NDA, in conjunction with other relevant Canadian laws, already meets the objectives underlying the Subcommittee's recommendations.

Regarding the proposal to require the CSE Commissioner to review interception activities for compliance with the *Charter* and *Privacy Act*, paragraph 273.63(2)(a) of the NDA already states that the Commissioner has a duty to review all of the activities of CSE to ensure that they are in compliance with the law. Similarly, as with any federal institution,

[6] [2002] 4 S.C.R. 3.
[7] [2004] 2 S.C.R. 248.

the activities of CSE are automatically required to conform to the *Charter*, *Privacy Act* and any other applicable legislation, and making specific reference to this in the case of CSE might actually weaken this fundamental principle in its application to other institutions for which such a reference was not made. Finally, with respect to legal issues of interpretation raised by the former CSE Commissioner, CSE is working with Department of Justice officials to address these issues, with a view to bringing forward proposed legislative amendments in due course.

G. THE *SECURITY OF INFORMATION ACT* (RECOMMENDATIONS 48 - 50)

Part 2 of the *ATA* enacted the *Security of Information Act* (*SOIA*), replacing the *Official Secrets Act*. Section 4 of the older Act was included in the SOIA, essentially without amendment. The *SOIA* focuses on conduct related to information security, such as espionage, that is or is likely to be harmful to Canada. It takes into account not only governments of traditional states, but also new actors such as governments-in-waiting, governments in exile and other foreign powers, as well as terrorist groups. Section 4 deals with the wrongful communication, use, reception, retention and failure to take reasonable care of certain government information.

In October 2006, sections 4(1)(a), 4(3) and 4(4)(b) of the SOIA were declared unconstitutional by the Ontario Superior Court of Justice in *Juliet O'Neill and The Ottawa Citizen* v. *the Attorney General of Canada*.[8] After careful consideration, the Attorney General of Canada decided not to appeal the decision.

The Government has previously indicated that it will consider legislative options to reform section 4; in that process it will bear in mind the comments of the Subcommittee and the recommendations made by witnesses who appeared before it.

The CSIS *Public Report* (2004-2005) demonstrates the continued necessity of the SOIA. For example, in considering the current threat environment, CSIS observes that terrorism is the most serious security threat. Various threats to Canada are cited, including the continued intimidation and exploitation by foreign entities and terrorist groups of

[8] 2006 CANLII 35004 (Ont.S.C.), Court File No. 11828, 2006-10-19.

Canada's immigrant and expatriate communities; the threat of cyber-attacks against private-sector and government targets; attempts by foreign entities and terrorist groups to acquire more lethal weapons, including chemical, biological, radiological and nuclear devices; spying and economic espionage. Offences in the Act address these concerns, as does the definition of "harms to Canadian interests" (also known as a purpose "prejudicial to the safety or interests of the State") in section 3 of the SOIA.

Regarding section 3 of the Act, the Government believes that moving the section under the "Interpretation" heading would improve the organization of the Act. Concerning the question of whether the list of purposes prejudicial to the safety or interests of the State in section 3 should be read as an indicative list or an exhaustive definition, the Government points out that section 3 is intended to be an exhaustive definition. The definitional nature of the present list operates as a safeguard. It allows persons to know what specific types of activities will be caught by the Act, thereby increasing *Charter* conformity. The Government does not believe that the provision should be expanded or made open-ended. Section 3 was designed to clearly identify harms from which Canada merits protection under the Act, including terrorist activity, interference with critical infrastructure, and the development of weapons of mass destruction in contravention of international law. In this way, the definition improved upon the former *Official Secrets Act* by providing greater clarity. The Government takes note of the Subcommittee's observation about the reference to "...any other purpose prejudicial to the safety or interests of the State..." in section 5, and will examine whether this wording is still necessary.[9]

H. THE *IMMIGRATION AND REFUGEE PROTECTION ACT*: SECURITY CERTIFICATES (RECOMMENDATIONS 51 - 52)

The Government shares the Subcommittee's view that the security certificate process is necessary to fulfill the obligation of democratic state institutions to protect themselves from being undermined and attacked. As the Subcommittee noted, great efforts have been made to balance, on the one hand, the need to protect Canadian society and, on the other,

[9] See Section A of the Government Response for a discussion of the Subcommittee's recommendation to amend the offence of harbouring and concealing in section 21 of the SOIA.

the rights of those subject to the process. The Subcommittee has suggested that more needs to be done to assure individual rights and freedoms in the security certificate process. On February 23, 2007, the Supreme Court of Canada issued its decision in the *Charkaoui v. Canada (Citizenship and Immigration)*[10] case and held that the Government could do more to protect the rights of the individual during the process used to determine if a security certificate is reasonable. Specifically, the Court endorsed the development of a model which included an independent agent. The Government accepts the decision of the Supreme Court and notes that many of the principles set forth in that decision were shared by this Subcommittee. The Government also notes that the Supreme Court suspended the effect of its decision for one year to allow the Government to develop legislation.

The Subcommittee also recommended limiting the evidence used when assessing a security certificate. It expressed the view that allowing only evidence which is "reliable" as well as "appropriate" would help render evidence obtained by torture inadmissible. The Government supports the proposed amendment. The Government also notes that, pursuant to subsection 269.1(4) of the *Criminal Code*, the contents of any statement obtained as a result of the commission of the *Criminal Code* offence of torture (section 269.1) is already inadmissible in evidence in any proceedings over which Parliament has jurisdiction.

In relation to the recommendation that an application to the Minister of Citizenship and Immigration for protection be allowed only after a security certificate has been found to be reasonable by a Federal Court judge, the Government agrees with the stated objective of making the process more expeditious and will examine methods to do so.

I. THE USE OF SPECIAL ADVOCATES (RECOMMENDATIONS 53 - 56)

The Government intends to address the decision of the Supreme Court in *Charkaoui*, and is currently reviewing how best to meet the principles established by the Supreme Court, with a view to creating legislation to be placed before Parliament as soon as possible. It

[10] 2007 SCC 9, 23 February 2007, Docket Nos. 30762, 30929, 31178.

will take the recommendations of the Subcommittee into account as it studies the possibility of establishing a special advocate role in the security certificate process. The Government will be guided by the need to ensure procedural fairness and to safeguard rights and freedoms under the *Charter*, consistent with the direction received from the Supreme Court.

There remain a number of challenges and considerations related to whether to introduce a special advocate for all *in camera, ex parte* proceedings, which involve the limited disclosure of information and evidence. Not all processes engage the *Charter* rights of individuals as in the *Charkaoui* case or to the same extent as in that case. Some of these issues have arisen in other litigation, such as the challenge to section 38 of the CEA in *R.* v. *Khawaja*, and in other processes such as the Air India Inquiry.

At the present time, the Government believes that further study of the use of special advocates in other processes is required.

J. REVIEW AND OVERSIGHT (RECOMMENDATIONS 57 - 60)

Canada's national security laws and the national security activities of federal government departments and agencies are vital and necessary to safeguarding our personal and collective safety and security. Many activities can and do have implications regarding the privacy of Canadians and the fundamental rights and freedoms guaranteed under the *Charter*. Safeguarding these fundamental aspects of Canadian life is one reason why effective review is so important. Ensuring that laws and practices remain effective and up to date, while at the same time striking an appropriate balance, requires ongoing vigilance at all levels, up to and including Parliament. The Subcommittee recommended that the Government proceed with legislation to establish a National Security Committee of Parliamentarians responsible for the review of national security matters and that it be called upon to conduct a further comprehensive review of the ATA after a fixed period.

The Government supports the principle that ongoing scrutiny of all of Canada's laws and practices relating to national security matters is essential, but has yet to determine that a review process based on fixed time periods and the fixed scope of the omnibus package of the ATA is the best way to proceed. To some extent, the ATA as a package can be seen as an artificial construct. It was a legislative package composed of new enactments and amendments to existing legislation based on the security needs of Canada that were identified when it was enacted in 2001. Some national security matters pre-date the 2001 amendments and are not part of the ATA. Other issues did not arise until after 2001 and have been addressed by legislative and other measures adopted since then. For example, changes to Canada's aviation security laws were made in the *Public Safety Act, 2002*. The constituent elements of the ATA are part of a larger and still-evolving national security legal framework. The need for a broader and more general review process is demonstrated by the fact that, in conducting the present reviews, Parliamentarians have felt it necessary to include elements of the IRPA and other measures that were outside of the scope of the original 2001 legislative package.

Elements of the ATA enacted or amended more than seventeen individual statutes, which raise other concerns. In many of these, the elements established by the ATA represent only a small part of a much larger picture. The statutes which contain them can be subject to other Parliamentary reviews and will evolve independently. This creates the potential for overlapping reviews and duplication of effort, and increasingly broad and unfocused proceedings, if future reviews are based on the framework of the ATA as opposed to the thematic nature of the subject matter and the issues that arise from time to time.

The Government believes that there is no simple solution to these questions, but that various forms of review are essential to ensure that Canada's national security laws and practices safeguard both security and civil liberties. For example, the review of specific statutes or provisions is routinely undertaken by the Government and Parliament in the normal course of making sure that Canada's laws are kept up-to-date and responsive to the needs of Canadians. The Government generally believes that such reviews should be

conducted when they are needed, as opposed to having a pre-set timetable. Some specific elements may require attention sooner, and others later, and the overall national security legal framework is broad enough that it may not be practicable or desirable to review all of it at the same time in a single process. As well, the review of the practices of the officials and agencies who administer the legislation is a matter for specialized review bodies accountable to Parliament and the Government is presently considering other recommendations in respect of some of these mechanisms.

The Government will propose an approach to national security review that will meet the basic objectives set out in the second report of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar and is considering options for an enhanced role for Parliamentarians as a key part of these proposals for an improved national security review framework.

The Government believes that the initial comprehensive review of the ATA five years after its enactment has been a positive and useful exercise. Parliamentarians have an important role to play in ensuring that Canada's statutes are kept up to date and effective and that the work of government departments and agencies is carried out in the best manner possible to meet the needs and expectations of Canadians. The Government is committed to strong and clear accountability as well as maximum transparency.

K. DRAFTING AND TECHNICAL RECOMMENDATIONS

The Subcommittee also recommended a number of technical and drafting changes throughout the ATA. The use of language and specific constructions in Canadian statutes is a technical matter and the Government is concerned that changes to terminology or structure in one provision could have the unintended consequence of affecting the judicial interpretation of others. For example, changes to the structure of the definition of "terrorism offence" might have an effect on interpretation of the definition of "criminal organization offence", which has a parallel structure. In some cases, provisions which implement international legal obligations may depart from Canadian drafting practice in

order to incorporate language or structure which reflects the international legal instruments concerned, thereby ensuring that Canada will be seen to be in conformity with those instruments. The Government has referred to the legislative drafters the recommendations which suggest drafting changes, technical changes or specific formulations and their advice will be reflected in any future amendments to the legislation.

ANNEX: RECOMMENDATIONS CONTAINED IN THE FINAL REPORT OF THE HOUSE OF COMMONS STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY SUBCOMMITTEE ON THE REVIEW OF THE *ANTI-TERRORISM ACT*

RECOMMENDATION 1

The Subcommittee recommends that the definition of "terrorist activity" contained in section 83.01(1) of the *Criminal Code* not be amended.

RECOMMENDATION 2

The Subcommittee recommends that the *Criminal Code* be amended to make it an offence to glorify terrorist activity for the purpose of emulation. Any such amendment should require the consent of the provincial attorney general to a prosecution, require the prosecution to prove that the accused intended to encourage emulation by the glorification of terrorist activity, and make available to the accused special defences similar to those included in section 319(3) of the Code.

RECOMMENDATION 3

The Subcommittee recommends that section 83.18 of the *Criminal Code* be amended so as to ensure that counsel providing legal services to those accused of terrorism offences can properly act on their behalf without fear of being charged themselves with terrorism offences.

RECOMMENDATION 4

The Subcommittee recommends that, unless the context dictates otherwise, the words "the Government of Canada or of a province" be replaced by the words "any government in Canada" throughout the provisions enacted or amended by the *Anti-terrorism Act*.

RECOMMENDATION 5

The Subcommittee recommends that the words "a person" and "the person" be replaced, respectively, by the words "an entity" and "the entity" in clause (*b*)(i)(B) of the definition of "terrorist activity" in section 83.01 of the *Criminal Code*.

RECOMMENDATION 6

The Subcommittee recommends that the words "an indictable offence under this or any other Act of Parliament where the act or omission constituting the offence also constitutes" be removed from paragraph (*c*) of the definition of "terrorism offence" in section 2 of the *Criminal Code*.

RECOMMENDATION 7

The Subcommittee recommends that the words "an offence under this Act for which the maximum punishment is imprisonment for five years or more, or an offence punishable under section 130 that is an indictable offence under the *Criminal Code* or any other Act of Parliament, where the act or omission constituting the offence also constitutes" be removed from paragraph (*c*) of the definition of "terrorism offence" in section 2(1) of the *National Defence Act*.

RECOMMENDATION 8

The Subcommittee recommends that the words "commit (i) a terrorism offence, or (ii) an act or omission outside Canada that, if committed in Canada, would be a terrorism offence" be replaced by "carry out a terrorist activity" in paragraphs 83.18(3)(*c*) and (*e*) of the *Criminal Code*.

RECOMMENDATION 9

The Subcommittee recommends that the words "facilitate or" be added before the first instance of the words "carry out" in sections 83.21(1) and 83.22(1) of the *Criminal Code*.

RECOMMENDATION 10

The Subcommittee recommends that the words "Every person" be replaced by the words "Every one" in the English versions of sections 83.21(1) and 83.22(1) of the *Criminal Code*.

RECOMMENDATION 11

The Subcommittee recommends that the words "any person" and "the person" be replaced, respectively, by the words "any entity" and "the entity" in sections 83.21(1), 83.21(2)(*c*) and (*d*), 83.22(1), and 83.22(2)(*c*) and (*d*) of the *Criminal Code*.

RECOMMENDATION 12

The Subcommittee recommends that section 83.23 of the *Criminal Code* be replaced by the following:

> "Every one who knowingly harbours or conceals any person whom he or she knows to be a person who
>
> (*a*) has carried out a terrorist activity, or
>
> (*b*) is likely to carry out a terrorist activity, for the purpose of enabling the person to facilitate or carry out any terrorist activity, is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years."
>
> Further, the word "cache" should be replaced by the word "recèle" in the French version of the section.

RECOMMENDATION 13

The Subcommittee recommends that the *Criminal Code* be amended to provide that every one who knowingly participates in a terrorist activity is guilty of an indictable offence and liable to imprisonment for up to life.

RECOMMENDATION 14

The Subcommittee recommends that the words "in addition to any penalty imposed for the commission of the original indictable offence" be added at the end of section 83.2 of the *Criminal Code*.

RECOMMENDATION 15

The Subcommittee recommends that section 83.25 of the *Criminal Code* be amended so that the Attorney General of Canada is required to make an application to a court in order to commence proceedings in a territorial division that would not be the one normally

used, or continue them in a different territorial division in Canada after they have already been commenced elsewhere in Canada. Any such amendment should set out the acceptable reasons for choosing a different location for the proceedings and the factors to be considered by the court in considering the application.

RECOMMENDATION 16

The Subcommittee recommends that section 83.1 of the *Criminal Code* be amended so as to exempt from its requirements legal counsel or law firms when they are providing legal services and not acting as financial intermediaries.

RECOMMENDATION 17

The Subcommittee recommends that section 83.08 of the *Criminal Code* be amended to allow for a due diligence defence.

RECOMMENDATION 18

The Subcommittee recommends that the words "wilfully and" be removed from section 83.02 of the *Criminal Code*.

RECOMMENDATION 19

The Subcommittee recommends that the words "without lawful justification or excuse" be added after the words "directly or indirectly" in section 83.03 and after the word "who" in section 83.04 of the *Criminal Code*.

RECOMMENDATION 20

The Subcommittee recommends that the words "a person" be replaced by the words "an entity" in the opening words of section 83.03 of the *Criminal Code*, and that the word "person" be replaced by the word "entity" in paragraph (*a*).

RECOMMENDATION 21

The Subcommittee recommends that the words "satisfy themself" be replaced by the words "be satisfied" in the English version of section 83.08(2) of the *Criminal Code*.

RECOMMENDATION 22

The Subcommittee recommends that the second instance of the word "and" be replaced by the word "or" in the opening words of subsection 83.1(1) of the *Criminal Code*, and that subsection 83.12(2) be repealed.

RECOMMENDATION 23

The Subcommittee recommends that consideration be given to further integrating the terrorist entity listing regimes established under the *Criminal Code*, the *Regulations Implementing the United Nations Resolution on the Suppression of Terrorism*, and the *United Nations Al Qaida and Taliban Regulations* insofar as the departmental administration, applicable test for inclusion, and legal consequences of listing are concerned.

RECOMMENDATION 24

The Subcommittee recommends that section 83.05 of the *Criminal Code* be amended so that, when a listed entity wishes to have an initial decision to list reviewed, it is not required to make an application to the Minister of Public Safety and Emergency Preparedness under subsection (2), but may instead apply directly to a court under subsection (5).

RECOMMENDATION 25

The Subcommittee recommends that section 83.05 of the *Criminal Code* be amended so that, when a listed entity applies to no longer be a listed entity in accordance with subsections (2) or (8), the Minister of Public Safety and Emergency Preparedness must make a recommendation within 60 days, failing which he or she is deemed to have decided to recommend that the applicant be removed from the list. Further, any recommendation or deemed recommendation on the part of the Minister should expressly be referred to the Governor in Council, which is to make a final decision within 120 days of the entity's application, failing which the entity is deemed to be removed from the list.

RECOMMENDATION 26

The Subcommittee recommends that section 83.05 of the *Criminal Code* be amended so that, on each two-year review of the list of entities under subsection (9), it is clear that the Governor in Council has the final decision as to whether or not an entity should remain a listed entity. Further, the decision should be made within 120 days of the commencement of the review, failing which the entity is deemed to be removed from the list.

RECOMMENDATION 27

The Subcommittee recommends that the *Charities Registration (Security Information) Act* be amended so that the Federal Court judge, to whom a certificate is referred, shall not find the certificate to be reasonable where an applicant or registered charity has established that it has exercised due diligence to avoid the improper use of its resources under section 4(1).

RECOMMENDATION 28

The Subcommittee recommends that, in consultation with the charitable sector, the Canada Revenue Agency develop and put into effect best practice guidelines to provide assistance to applicants for charitable status and registered charities in their due diligence assessment of donees.

RECOMMENDATION 29

The Subcommittee recommends that section 8(2) of the *Charities Registration (Security Information) Act* be amended to allow for an appeal to the Federal Court of Appeal of a decision by a Federal Court judge that a referred certificate is reasonable.

RECOMMENDATION 30

The Subcommittee recommends that the words "the applicant or registered charity knew or ought to have known that" be added after the words "*Criminal Code* and" in paragraphs 4(1)(*b*) and (*c*) of the *Charities Registration (Security Information) Act*.

RECOMMENDATION 31

The Subcommittee recommends that the words "terrorist activities" be replaced by the words "a terrorist activity," and that the words "activities in support of them" be replaced by the words "an activity in support of a terrorist activity", in paragraphs 4(1)(*b*) and (*c*) of the *Charities Registration (Security Information) Act*.

RECOMMENDATION 32

The Subcommittee recommends that the words "at that time, and continues to be," be removed from section 4(1)(*b*) of the *Charities Registration (Security Information) Act*.

RECOMMENDATION 33

The Subcommittee recommends that subsections 5(3) and (4) of the *Charities Registration (Security Information) Act* be repealed and that the Act be amended so that, beginning from the time that an applicant or registered charity is being investigated for allegedly making resources available to a terrorist entity, its identity shall not be published or broadcast, and all documents filed with the Federal Court in connection with the reference of the certificate shall be treated as confidential, unless and until the certificate is found to be reasonable and published under section 8.

RECOMMENDATION 34

The Subcommittee recommends that section 11 of the *Charities Registration (Security Information) Act* be amended to make it clear that an applicant or registered charity may apply for review of a decision made under paragraph 10(5)(*b*)(i), even if it has already applied for review of a decision made under paragraph 10(5)(*a*).

RECOMMENDATION 35

The Subcommittee recommends that section 38.13(9) of the *Canada Evidence Act* be amended so that a certificate expires ten years after it has been issued.

RECOMMENDATION 36

The Subcommittee recommends that section 38.131(11) of the *Canada Evidence Act* be repealed and that there be established a right to apply to the Supreme Court of Canada for leave to appeal the decision of a Federal Court of Appeal judge who has conducted a judicial review of a certificate issued by the Attorney General of Canada. Such an appeal should be considered by a reduced panel of three members of the Supreme Court.

RECOMMENDATION 37

The Subcommittee recommends that the *Canada Evidence Act* be amended to require the Attorney General of Canada to table in Parliament an annual report setting out the usage of section 38.13 certificates and section 38.15 fiats.

RECOMMENDATION 38

The Subcommittee recommends that section 38.04 of the *Canada Evidence Act* be amended to require the Attorney General of Canada, with respect to information about which notice was given from a party to proceedings under any of subsection 38.01(1) to (4), to apply to the Federal Court for an order with respect to disclosure of the information in every case where, except by agreement with the party, the Attorney General does not permit full disclosure without conditions.

RECOMMENDATION 39

The Subcommittee recommends that the government prepare written guidelines, and implement appropriate review mechanisms, to assist designated entities in fulfilling their duty to prevent the disclosure of sensitive or potentially injurious information and to notify the Attorney General of Canada under section 38.02(1.1) of the *Canada Evidence Act*.

RECOMMENDATION 40

The Subcommittee recommends that the word "may" be replaced by the word "shall" in subsections 37(4.1), 37(5), 38.06(1) and 38.06(2) of the *Canada Evidence Act*.

RECOMMENDATION 41

The Subcommittee recommends that subsection 37(7) of the *Canada Evidence Act* be replaced by the following:

> "An order of the court that authorizes disclosure does not take effect until
>
> *(a)* the time provided or granted to appeal the order has expired, or
>
> *(b)* a judgment of an appeal court has confirmed the order and the time provided or granted to appeal the judgment has expired, or no further appeal is available."

RECOMMENDATION 42

The Subcommittee recommends that the *Canada Evidence Act* be amended so that an order authorizing disclosure under subsections 38.06(1) or (2) does not take effect until (*a*) the time provided or granted to appeal the order has expired, or (*b*) a judgment of an appeal court has confirmed the order and the time provided or granted to appeal the judgment has expired, or no further appeal is available.

RECOMMENDATION 43

The Subcommittee recommends that section 37.21 of the *Canada Evidence Act*, which was repealed in 2004, be re-enacted.

RECOMMENDATION 44

The Subcommittee recommends that section 273.65(8) of the *National Defence Act* be amended to require the Commissioner of the Communications Security Establishment to review the private communication interception activities carried out under ministerial authorization to ensure they comply with the requirements of the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*, as well as with the authorization itself (as already required).

RECOMMENDATION 45

The Subcommittee recommends that section 273.66 of the *National Defence Act* be amended to require the Communications Security Establishment to only undertake activities consistent with the *Canadian Charter of Rights and Freedoms* and the *Privacy*

Act, in addition to the restraints on the exercise of its mandate already set out in that section.

RECOMMENDATION 46

The Subcommittee recommends that the words "The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment" be replaced by the words "The Governor in Council may appoint a Commissioner of the Communications Security Establishment, who shall be a supernumerary judge or a retired judge of a superior court," in section 273.63(1) of the *National Defence Act*.

RECOMMENDATION 47

The Subcommittee recommends that the word "anywhere" be added after the word "Canadians" in paragraph 273.64(2)(*a*) of the *National Defence Act*.

RECOMMENDATION 48

The Subcommittee recommends that the heading "Offences", preceding section 3 of *Security of Information Act,* be removed.

RECOMMENDATION 49

The Subcommittee recommends that section 3 of the *Security of Information Act* be amended, for example through use of the word "includes," so that the list of what constitutes a purpose prejudicial to the safety or interests of the State is clearly non-exhaustive.

RECOMMENDATION 50

The Subcommittee recommends that subsection 21(1) of the *Security of Information* be replaced by the following:

> "Every one commits an offence who knowingly harbours or conceals a person whom he or she knows to be a person who
>
> (i) has committed an offence under this Act, or

(ii) is likely to commit an offence under this Act, for the purpose of enabling the person to facilitate or commit an offence under this Act."

Further, the word "héberge" should be replaced by the word "recèle" in the French version of the section.

RECOMMENDATION 51

The Subcommittee recommends that section 78(j) of the *Immigration and Refugee Protection Act* be amended by adding the words "reliable and" before the word "appropriate".

RECOMMENDATION 52

The Subcommittee recommends that sections 79, 81, 112, and other provisions of the *Immigration and Refugee Protection Act* be amended so as to allow for an application to the Minister of Citizenship and Immigration for protection only after a security certificate has been found by a Federal Court judge to be reasonable.

RECOMMENDATION 53

The Subcommittee recommends that a Panel of Special Counsel be established by the government in consultation with the legal profession and the judiciary. Counsel appointed to the Panel should be security-cleared and have expertise relevant to issues related to the listing of terrorist entities under the *Criminal Code*, the de-registration of registered charities and denial of charitable status to applicants under the *Charities Registration (Security Information) Act*, applications for the disclosure of information under the *Canada Evidence Act*, and the security certificate process under the *Immigration and Refugee Protection Act*. The functions of Special Counsel should be to test the need for confidentiality and closed hearings, and to test the evidence not disclosed to a party.

RECOMMENDATION 54

The Subcommittee recommends that counsel from the Panel should be appointed at the request of a judge presiding over a hearing or by a party excluded from an *ex parte*, *in camera* proceeding.

RECOMMENDATION 55

The Subcommittee recommends that the Panel should have the capacity to provide counsel appointed to it with the investigative, forensic, and other tools they require to effectively carry out the functions assigned to them.

RECOMMENDATION 56

The Subcommittee recommends that counsel appointed to the Panel be provided with the necessary training to allow them to effectively carry out the functions assigned to them.

RECOMMENDATION 57

The Subcommittee recommends that section 145 of the *Anti-terrorism Act* be amended so as to require that there be another comprehensive review of its provisions and operation, to be commenced no later than December 31, 2010 and completed no later than December 31, 2011.

RECOMMENDATION 58

The Subcommittee recommends that Bill C-81 from the 38th Parliament, the proposed *National Security Committee of Parliamentarians Act*, or a variation of it, be introduced in Parliament at the earliest opportunity.

RECOMMENDATION 59

The Subcommittee recommends that the mandate of the proposed National Security Committee of Parliamentarians be clarified so as to ensure that in carrying out its activities in relation to departments and agencies in respect of national security, it is empowered to conduct compliance audits in relation to the *Anti-terrorism Act*.

RECOMMENDATION 60

The Subcommittee recommends that the mandate of the proposed National Security Committee of Parliamentarians be clarified so as to ensure that it can carry out the next comprehensive review of the *Anti-terrorism Act* under an amended section 145 of that Act, failing which the review should be carried out by a committee of Parliament.