Mr. Robert Oliphant, M.P.
Chair
Standing Committee on Public Safety and National Security
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Oliphant,

On behalf of the Government of Canada, we are pleased to respond to the Ninth Report of the Standing Committee of Public Safety and National Security, entitled, *Protecting Canadians and their Rights: A New Road Map for Canada's National Security.*

We would like to take this opportunity to commend the Committee for undertaking this important study, and to express our appreciation to the experts who appeared before the Committee to share their views. The Report provides valuable insights and puts forward constructive recommendations to continue improving Canada's national security framework. As identified in the Report, the Government's measures to ensure the safety and security of Canadians must also respect the constitutionally protected rights and freedoms of Canadians. In the Report, references to accountability and transparency were highlighted throughout, and the Government is working towards enhancing both pillars within its national security framework.

The mandate letters of the Minister of Public Safety and Emergency Preparedness and the Minister of Justice and Attorney General of Canada direct us to work together to repeal the problematic elements of the former Bill C-51, and to introduce legislation that strengthens accountability and national security. In this respect, the Government launched a broad public consultation on Canada's national security framework that took place in 2016. In general, there is considerable alignment between the Committee's recommendations and current and planned Government initiatives to enhance Canada's national security framework, while safeguarding rights and freedoms.

Please find below the Government Response to the Parliamentary Committee's Report, organized along key themes identified in the Report:

Countering Radicalization to Violence

(Pertaining to recommendations 2, 3, 4, 5)

The Government announced $35 million over five years, and $10 million per year ongoing to create an Office for community outreach and countering radicalization to violence (the Office). As a centre of excellence, the Office will provide national leadership on Canada's response to radicalization to violence, coordinate talent and expertise, provide support to municipal, community and grassroots efforts, and enhance the evidence base on this issue. Its goal is to support the prevention of radicalization to violence of all kinds, regardless of where it originates.

The Government is committed to ensuring that our continuing efforts in this area are informed by extensive new research and input from a wide range of stakeholders. As part of this commitment, the Office will be engaging broadly across the country in 2017 to advance a national strategy on countering radicalization to violence (CRV) that is representative of diverse Canadian views. To this end, the Office will actively engage with Canada's diverse communities, experts, academia, key sectors (e.g., first responders, education, police, social services, health services, private sector) and various groups (e.g., women, youth, faith-based).

As part of its role as a centre of excellence, the Office will both develop its own in-house expertise to help produce and mobilize a greater evidence base, and support efforts led by other organizations and initiatives. The latter will include collaboration with other government agencies as they continue building evidence-based CRV tools, as well as with initiatives funded elsewhere in the federal government, such as through Defence Research and Development Canada's Canadian Safety and Security Program (CSSP), and the Social Sciences and Humanities Council of Canada (SSHRC). A notable example of research supported by both CSSP and SSHRC is the wide range of studies led by the Canadian Network for Research on Terrorism, Security, and Society, a group with which the Office is already collaborating. In addition, Provincial and Territorial Ministries are also investing in CRV research, with recent calls for proposals in both Quebec and Ontario, and the Office will work to complement such efforts in developing and sharing expertise.

Similar to the Office, a range of departments and agencies are actively involved as leads or lead partners in major initiatives for long-term research and professional development, to address a broader range of new and evolving threats. Examples include the Academic Outreach Program at the Canadian Security Intelligence Service, the SERENE-RISC Smart Cybersecurity Network supported by the Networks of Centres of Excellence Canada federal funding program, and ongoing investments by CSSP to partner with lead agencies responsible for national security on long-term research and development to address current and emerging security threats. Additionally, the Communities at Risk: Security Infrastructure Program (SIP), designed to help communities at risk of hate crimes, has streamlined its submission process to enhance flexibility and accessibility to the program. In Budget 2017, new funding of $5.0 million over five years has been allocated, starting in 2017-18, in support of SIP. Such initiatives bring together experts and

practitioners from within and outside government, aim to address both current and emerging threats, and will continue to have a central role to play in the development and application of knowledge.

National Security Review, Oversight and Accountability

(Pertaining to recommendations 1, 6, 7, 8, 9, 10)

The former Bill C-51, the *Anti-terrorism Act, 2015* (ATA, 2015), was introduced in January 2015 to address gaps in the national security framework and was meant to complement existing measures. The ATA, 2015 resulted in controversy and criticism from a significant number of Canadians, many pointing to the fact that given the speed of its implementation, there was limited opportunity to explain how it worked or to engage Canadians in meaningful discourse on the important issues it raised. In light of these concerns, the Government is committed to enhancing accountability and transparency in the national security framework.

Accountability and transparency were central issues in the 2016 Consultation on National Security, with a majority of participants considering the current system of accountability to be inadequate. Most of those who were prepared to accept some new powers for law enforcement and national security agencies insisted that there be additional oversight and transparency, and more checks and balances. The Government agrees with the importance of improving accountability in the national security framework in light of the increasingly interconnected activities of national security agencies.

The Government would like to echo the Committee that the creation of a National Security and Intelligence Committee of Parliamentarians (NSICoP), as envisaged by Bill C-22, is a first step toward increasing the accountability of the security agencies. As such, the government is proposing to introduce legislation that would replace the current system of national security review, with dedicated review bodies that scrutinize the activities of a single agency, with one body, the National Security and Intelligence Review Agency (NSIRA). NSIRA would have the authority and resources to review all national security and intelligence activities across the government in an integrated and comprehensive manner.

The NSIRA would address the current "siloed" approach to national security review by reviewing the activities of all departments, agencies and parent Crown corporations insofar as they are related to national security or intelligence. This would include national security and intelligence agencies such as the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE), as well as the relevant activities of many other departments and agencies with national security responsibilities, including the Royal Canadian Mounted Police (RCMP) and the Canada Border Services Agency (CBSA). The NSIRA would only review the RCMP and CBSA's activities related to national security and intelligence.

In addition to enhancing accountability in the national security framework, the Government is committed to greater transparency. It is important for Canada's national security framework to

be accountable to Canadians, and for Canadians to be able to develop confidence in Government's fulfillment of its national security responsibilities. In this respect, the Government is proposing to establish a National Security Transparency Commitment to be applied across Canada's national security framework. The implementation of this Transparency Commitment would support citizens in understanding *what* the Government does to protect national security and inform Canadians' consideration of *how* those efforts are consistent with Canadian values and *why* the work is effective and important.

Public Safety Canada intends to establish an advisory group on national security transparency. This group, which will seek to include civil rights advocates, experts in the fields of security, intelligence and open government, as well as other stakeholders, would be consulted on their priorities for enhancing national security transparency and potential approaches to implementing the principles. Input from the Cross-Cultural Roundtable on Security will also be sought.

Disruption Powers of CSIS

(Pertaining to recommendations 11, 12, 13, 14, 15)

The ATA, 2015 included amendments to the *Canadian Security Intelligence Service Act* (*CSIS Act*) to provide CSIS with new threat reduction authorities. Following these amendments, there was public and stakeholder criticism of the breadth and vagueness of CSIS's new powers. These criticisms were echoed during the 2016 Consultation on National Security. The Government is proposing to introduce legislative amendment that would narrow the scope of the CSIS threat reduction warrant regime and introduce a range of new safeguards for CSIS's threat reduction activity in general to ensure compliance with the *Canadian Charter of Rights and Freedoms* (the *Charter*).

The Government is proposing that the threat reduction warrant regime in the *CSIS Act* be revised to strengthen its compliance with the *Charter*. The current open-ended warrant regime would be replaced by a clear set of specific powers needed to confront the evolving threats facing Canada. This would reduce the *Charter* risk while still providing CSIS with the tools it needs to respond to national security threats. Additionally, our Government agrees with the Committee that section 12.1(3) of the *CSIS Act* be repealed and is proposing legislative changes to ensure that CSIS cannot violate or contravene the *Charter*.

The Government's proposed alternative would more clearly define the scope of CSIS's powers by replacing the current open-ended warrant regime with a specific list of threat reduction powers that CSIS could employ, with judicial authorization. In doing so, concerns over the scope of disruption activities would be addressed by reducing disruption under warrant to a closed list of possible measures. The changes above would bring the threat reduction warrant regime closer to CSIS's long-standing intelligence collection warrant regime, which also requires a warrant to use a specified list of powers.

In terms of CSIS's threat reduction mandate, the Government is proposing to introduce additional safeguards to address public concern that the effects of threat reduction measures could "spill over" onto people not engaged in hostile acts. The Government is proposing new prohibitions, including prohibitions on the detention of individuals and on property loss or damage that could harm an individual. These new prohibitions would make clear that CSIS's threat reduction powers cannot be misused to take extreme and unacceptable measures.

To ensure that CSIS considers all other means of addressing threats and does not impede on police operations, the Government is proposing that CSIS be required by law to consider the other tools and powers available to other government departments and agencies (such as the RCMP) before taking measures to reduce a threat. This requirement would help to ensure that CSIS's threat reduction powers are used only when they represent the best and most appropriate tool for addressing the threat in question, and that they do not interfere with or hinder police investigations.

The Government is also committed to enhancing accountability and transparency of CSIS's disruption activities. The NSICoP will have the opportunity to comment on CSIS's use of its threat reduction powers in its annual public report. Further, CSIS would be required to automatically inform its independent review body, the Security Intelligence Review Committee (SIRC) or NSIRA (if proposed legislation is passed by Parliament) of all threat reduction measures it has taken. The review body could then review those measures at its discretion. SIRC (or NSIRA) would also gain the authority to inform the Attorney General, via the Minister of Public Safety and Emergency Preparedness, when it deems CSIS to have broken the law.

Law Enforcement Powers

(Pertaining to recommendations 16, 17, 18, 19, 20, 21)

The Government understands that terrorism cannot be eradicated by criminal law tools alone, and that early intervention methods as a means to address the threat of terrorist activity are crucial to Canada's whole-of-government approach to ensuring the safety and security of Canadians.

The Committee's recommendation that the power of preventive detention should be restricted to exceptional, narrowly-defined circumstances and be consistent with human rights standards appears to be directed at the power to detain a person under the recognizance with conditions power found in section 83.3 of the *Criminal Code*. That power is already subject to important safeguards, including judicial scrutiny and approval, as well as a proposed threshold increase. Under that power, a peace officer can detain a person without warrant for generally a maximum period of up to 24 hours but only in very narrow circumstances (e.g., in exigent circumstances). There is also an initial maximum 48-hour period of judicially-ordered detention, but such detention can only be ordered if a statutory ground of detention is met (that is, where necessary to ensure the person's appearance, the protection or safety of the public or to maintain confidence in the administration of justice). The period of detention can be extended

for up to another 48 hours twice by order of a judge (that is, up to a further maximum of 96 hours detention), but only where, in addition to satisfying the judge that a previously-mentioned statutory ground of detention has been met, that a peace officer also satisfies the judge that the investigation in relation to the person detained is being conducted diligently and expeditiously.

The Committee is also concerned that the current thresholds for the recognizance with conditions are too low. The current proposal seeks to increase this threshold.

With regards to the offence of advocating or promoting the commission of terrorism offences in general and that part of the definition of terrorist propaganda that refers to this offence, the Government is proposing to introduce legislative amendments that would clarify its scope. The offence is meant to be a form of counselling, so that the offence should be modelled on the criminal law governing counselling rather than the hate propaganda offence of willful promotion of hatred against an identifiable group. Accordingly, the Government is also proposing legislative amendments that would narrow the definition of "terrorist propaganda".

The Government is also committed to ensuring the continued protection of the right to freedom of expression and freedom of association, as prescribed in the *Charter*. Moreover the right to freedom of expression is recognized in a statutory clarification to the definition of "terrorist activity", which is a key element of the recognizance with conditions power.

The Government understands that terrorism cannot be eradicated by prosecutions alone. It is crucial to work with communities to prevent people, particularly youth, from being radicalized to violence.

Domestic Information Sharing

(Pertaining to recommendations 22, 23, 24, 25, 27)

The Government is committed to clarifying the scope and threshold of the *Security of Canada Information Sharing Act* (SCISA), through proposed legislative and non-legislative measures. Since coming into force in 2015, there continues to be confusion with respect to the SCISA in terms of its use and overall purpose. These concerns were reiterated through the 2016 Consultation on National Security. The Government is also responding to the report by the Standing Committee of Access to Information, Privacy, and Ethics (ETHI), entitled, *Safeguarding Canada's National Security while Protecting Canadians' Privacy Rights: Review of the Security of Canada Information Sharing Act (SCISA).*

Through the 2016 Consultation on National Security and the ETHI report, it was determined that the concerns raised stem partly from a lack of understanding of the legislation as drafted and from a lack of communication of the underlying need and purpose of the SCISA when it was first introduced. In order to address these concerns, and the recommendations made in the

Committee's report, the Government is proposing legislative amendments that would add more specificity to the disclosure threshold and would clarify other elements of the Act.

With respect to the scope of the SCISA (i.e., the definition of "activity that undermines the security of Canada), the Government is proposing that the list of illustrative activities be amended to include only those that would, in all cases, meet the threshold for disclosure (i.e., would always be an "activity that undermines the security of Canada") and explicitly prohibiting the sharing of information related to advocacy, protest, dissent and artistic expression activities at the disclosure stage unless they are carried out in connection with an "activity that undermines the security of Canada."

In addition to clarifying the scope of the SCISA, the Government is also proposing that the threshold provision be clarified, by going beyond "relevant", and specifying requirements for disclosure. These requirements would speak to the utility of the information (that it contribute to the recipient's national security jurisdiction) and the integrity of the information (must provide a statement on the reliability and accuracy), and would require that the impact on privacy not be more than is reasonably necessary in the circumstances.

To assist in the general understanding of the SCISA, the Government is also proposing that the legislation be re-named (in English) as "*The Security of Canada Information Disclosure Act*" to clarify the intent and purpose of the legislation – which has been a source of significant confusion amongst Canadians.

In response to concerns raised about accountability, a new provision is being proposed that would require institutions to maintain records with respect to all disclosures made under the Act and would specify the requirements for those records. In addition, institutions would be required to provide these records to the NSIRA (should proposed legislation be passed by Parliament).

Finally, the Government proposes that it increase transparency by building support capacity in the national security information-sharing process by establishing a Centre of Expertise for information sharing within the national security community. The Centre of Expertise would have a specific mandate to provide guidance on information-sharing authorities and best practices, with a focus on non-traditional national security institutions

The Government agrees that, given the sensitivity of the information being shared, an appropriate threshold for disclosing information must be upheld, while not impeding the information-sharing process.

International Information Sharing

(Pertaining to recommendation 28)

The Government is proposing that the Minister of Public Safety and Emergency Preparedness, the Minister of National Defence, and the Minister of Foreign Affairs develop a revised *Ministerial Direction (MD) on Information-Sharing with Foreign Entities* which would address the Committee's recommendation regarding ministerial directives concerning torture. This proposed MD would begin with a clear statement of Canadian values. It would explain the existing laws, including the *Criminal Code* and the *Charter*, and international obligations that govern the actions of security and law enforcement agencies when it comes to torture. The text would include a more straightforward and clear definition of substantial risk, and clearer procedures for handling incoming information versus outbound sharing.

Intelligence and Classified Information Used as Evidence

(Pertaining to recommendations 29, 30)

When national security information is involved, or potentially involved, in legal proceedings, it brings into play issues that are fundamental to justice, the rule of law and to the confidence that Canadians have in not only their system of justice but also the national security agencies mandated to protect Canadians from serious harm. This issue was raised in the the 2016 Consultation on National Security, and 71% of online respondents felt that *Canada Evidence Act* section 38 proceedings do not appropriately balance fairness and security, and 64% believed that a security-cleared lawyer should be used to represent an accused in closed legal proceedings.

Section 38 provides the framework for the disclosure and use of national security information in a broad range of legal proceedings. The process is a two-court system, known as a bifurcated process. Under section 38, a Federal Court judge must assess whether or not the disclosure would be injurious to international relations, national defence or national security. The process under section 38 is conducted in the Federal Court even though, for example, the information may relate to a proceeding in a different court.

In cases where national security information is involved, or potentially involved in legal proceedings, security-cleared lawyers can be appointed and can have a range of functions.

The Government is aware of the concerns with respect to the bifurcated process for criminal cases, as well as the important role security-cleared lawyers can, and do, play in certain proceedings and is assessing the viability of law reform in both these areas.

Passenger Protect Program

(Pertaining to recommendations 32, 34, 35, 36, 38)

The ATA, 2015 enacted the *Secure Air Travel Act* (SATA). Under SATA, the Government can use the Passenger Protect Program (PPP) to prevent individuals from boarding a flight if they pose a threat to transportation security, or are seeking to travel by air to commit certain terrorism offences. The PPP is an important element of Canada's national security framework and addresses the continued threat of individuals travelling abroad to engage in terrorism offences – known as "extremist travellers".

The Government is proposing legislative amendments to improve the PPP. These improvements would build on the Committee's recommendations, platform commitments, and are in line with responses the Government received from the 2016 Consultation on National Security.

Firstly, the Government is committed to implementing a redress mechanism to better deal with the issue of false positive matches to the SATA list. This commitment builds on previously implemented Government initiatives to improve the PPP. In 2016, the Government announced the creation of the Passenger Protect Inquiries Office (PPIO) as a first step to assist travellers who have experienced delays related to aviation security lists. Building on the PPIO, a redress mechanism would allow individuals experiencing travel delays, as a result of having the same or a similar name as a listed individual, to apply for a unique identification number to use at the time of a ticket purchase to clear their name in advance and prevent delays at the airport. The Government understands the frustration of those who have experienced issues related to the PPP, and is committed to a fast and efficient redress mechanism.

Secondly, and to carry out the Government's platform commitment to review all appeals by Canadians on the no-fly list, the Government is committed to enhancing procedural fairness regarding the PPP recourse process. Under SATA, a listed person who has been denied boarding may apply to the Minister of Public Safety and Emergency Preparedness to have their name removed from the list. Currently, the Minister may take up to 90 days to review and decide whether there are still reasonable grounds for a recourse applicant to be listed. The Government is proposing legislative amendments to reverse this "deemed decision" so that a recourse applicant's name would be automatically removed from the SATA list if a decision is not taken within a specified period of time. Because there are cases when delays are unavoidable, such as when agencies are waiting for information from foreign partners or when the applicant has requested more time to respond to the case against him/her, it is proposed that the Minister may extend the set decision period in certain circumstances.

Thirdly, the Government is committed to enhancing its dialogue with Canadians who have experienced travel delays as a result of the PPP. For example, parents whose young children have encountered travel delays due to false positive matches have posed questions as to why their children are 'listed' and how they can be removed. The Government is proposing to introduce an authority for the Minister of Public Safety and Emergency Preparedness that

would allow him or her to inform parents that the child is not in fact listed, and allow further disclosure once the Minister has informed a parent that their child is not on the SATA list. Disclosure to a parent would provide assurance to families that a child has not been mistakenly added to the SATA list.

While the Committee has recommended that the Government disclose the number of individuals on the SATA list to Parliament, the Government maintains that releasing the number of listed individuals would reduce the efficacy of the program, and create a reasonable risk of probable harm to national security. That said, the Government is looking into options that will enhance transparency related to the PPP, such as releasing materials that explain the main elements of the program and legislation, and how the Government interprets and implements that legislation in line with Canadian values, including those expressed by the *Charter*.

Investigative Capabilities in a Digital World

(Pertaining to recommendation 39)

The Government recognizes the importance and complexity of issues related to lawful access. Canadians remain highly engaged on these issues, as demonstrated by the 41,000 responses the Government received regarding the 2016 Consultation on National Security theme of "Investigative Capabilities in a Digital World". As technology and threats to our security continue to rapidly evolve, it is more important than ever to ensure that our security and law enforcement agencies are able to operate with modern tools. The Government will need to meet both the needs of investigators and Canadians' expectations of privacy in a digital world in in any future legislative proposals.

Basic subscriber information (BSI) was a prominent topic in the responses to the *Green Paper* consultations. Canadians and stakeholders raised privacy concerns around this issue, as they have in response to previous legislative proposals for access to BSI. Many believed that police should be required to obtain court orders in order to obtain BSI in all situations except for emergencies.

With regard to the matter of encryption, the Government has not proposed any changes to Canada's lawful access regime as it relates to this issue. It is in Canada's interest to ensure that encryption technologies remain robust and widely-used. Encryption has been essential for the growth of Canada's digital economy and is critical to safeguarding Canadians' cybersecurity and online privacy. While the spread of powerful encryption has created significant gaps for law enforcement and national security agencies, the Government does not consider legislative responses to these challenges to be viable. The Government continues to examine options to ensure departments and agencies have the resources necessary to gain access to decrypted data required to prevent terrorist incidents and address criminal activity.

Communications Security Establishment (CSE) Activities

(Aligned with recommendation 40)

With regard to recommendation 40, part of CSE's mandate is to provide technical and operational assistance. CSE may render this assistance in response to requests which federal security and law enforcement agencies make in the course of their lawful security intelligence and criminal investigations. The activities that CSE undertakes in response to such requests must conform to the lawful authorities of the requesting agency, including warrants.

Cyber Security

(Pertaining to recommendation 41)

The Government recently completed a Cyber Security Review as a means of taking stock of the existing measures to protect Canadians and Canadian critical infrastructure from cyber threats. The review was an opportunity to examine evolving threats in cyberspace as well as to understand and explore the ways that cyber security has become a driver of economic prosperity.

As part of this review, the Government initiated a public consultation process that sought the views of Canadians, the private sector, academia, and other informed stakeholders on cyber security. A range of comments were submitted, including ways in which the government can best serve the needs of the private sector and Canadians.

In addition to these consultations, an examination of the current cyber security strategies of international partners was conducted, in order to identify lessons learned and common practices. Internal discussions on important policy issues, operational issues and how government should better organize itself to deliver on its cyber security mandate also took place. Results of the external consultations and the various internal discussions will inform how Government should position itself to deliver policy and programs that will best support a cyber security strategy that is tailored to the needs of our nation.

In closing, and on behalf of the Government, we would like to thank the Standing Committee on Public Safety and National Security for its comprehensive Report. The Report will be a valuable resource as the Government moves forward with its commitment to addressing the problematic elements of the former Bill C-51 and introducing measures that enhance Canada's national security framework, while safeguarding rights and freedoms.

Yours sincerely,

The Honourable Ralph Goodale, P.C., M.P.
Minister of Public Safety
and Emergency Preparedness

The Honourable Jody Wilson-Raybould, P.C., Q.C., M.P.
Minister of Justice
and Attorney General of Canada