Mr. Blaine Calkins, M.P.
Chair
Standing Committee on Access to Information, Privacy and Ethics
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Calkins,

Pursuant to Standing Order 109 of the House of Commons and on behalf of the Government of Canada, we are pleased to respond to the report by the Standing Committee on Access to Information, Privacy and Ethics, entitled, *Safeguarding Canada's National Security while Protecting Canadians' Privacy Rights: Review of the Security of Canada Information Sharing Act (SCISA).*

We would first like to thank the Committee for undertaking this review of such an important piece of legislation in Canada's national security framework. In addition, we would like to express our appreciation to the experts who appeared before the Committee to provide their views and share their experiences in using the SCISA. The report by the Committee provides thoughtful and constructive recommendations to improve Canada's information sharing for national security purposes.

It is well known that national security institutions require information to detect, analyze, investigate and prevent threats and often times this requires multiple pieces of information from multiple different sources. Given today's national security environment, threats can evolve rapidly, therefore the appropriate tools need to be in place to ensure the timely and effective disclosure of information. The Air India Commission of Inquiry, the Auditor General and other commentators identified real and perceived barriers that were preventing Government officials from disclosing information for national security purposes. As such, the SCISA was created to provide a clear, explicit authority for Government of Canada institutions to disclose information for national security purposes. In particular, it provides a lawful authority for Government of Canada institutions to proactively disclose national security-relevant information to federal institutions with a national security jurisdiction or responsibilities and sends a clear signal that information may be disclosed to address national security threats.

The Committee's Report, the 2016 Consultation on National Security, and the Office of the Privacy Commissioner 2015-2016 Annual Report to Parliament have helped clarify for Canadians the purpose and scope of the Act. However, more work is needed to explain the SCISA's role in protecting our national security and its existing safeguards to protect privacy.

Moreover, the Government agrees with the Committee that changes are needed to improve the SCISA, particularly regarding clarifying its scope and requirements for disclosing information, as well as the need for greater direction and guidance on its use.

To this end, please find below the Government Response to the Parliamentary Committee's Report, organized along key themes identified through the recommendations:

Increased Transparency of the List of Designated Recipient Institutions

(Pertaining to Recommendations 1 & 2)

Schedule 3 of the SCISA currently allows 17 departments/agencies to receive information for national security purposes. Concerns have been raised as to why there are so many institutions included in the Act. The Government agrees with the Committee and the feedback received through the Consultation that a better explanation of the rationale for inclusion of each designated recipient institution is required. In response to these concerns:

- Deputy Heads would be asked to re-validate their institutions need to be a listed entity in Schedule 3, with the aim of ensuring that only institutions with clear national security jurisdiction or responsibilities will be included on the list;

- The Government would publish an overview of the national security jurisdiction and responsibilities of each recipient institution; and,

- We would make public which positions and/or directorates within the institution have been delegated by the Head of each institution to receive information, to further clarify that only areas dealing with national security matters, specifically institutions whose core mandate is not national security but which have national security responsibilities, are able to receive information under the SCISA.

Scope, Disclosure Threshold and Existing Information Management Authorities

(Pertaining to Recommendations 3-6 & 8-11)

Scope

The Committee expressed concern that the scope of the SCISA (i.e., the definition of "activity that undermines the security of Canada) is too broad. As such, stakeholders have asked for a narrowing of the definition or that the SCISA's definition be replaced by the definition found in the *CSIS Act* ("threats to the security of Canada"), which more clearly articulates which activities threaten Canada and is a more familiar and tested definition. The list of illustrative examples included in the SCISA has also raised questions about how the definition was to be applied, with some believing information collection authorities are expanded. And, finally, there were concerns that the Act could inhibit advocacy, protest, dissent and artistic expression.

To have value, the SCISA must cover all information that is needed for government institutions to carry out their national security responsibilities. These can range in scope from the Canada Border Services Agency's responsibility to provide integrated border services that support national security and public safety priorities to the Canadian Food Inspection Agency's responsibility to respond rapidly and effectively to food safety emergencies or threats to agricultural or forest biosecurity, including bioterrorism and agro-terrorism. An overly narrow scope could prevent important information from being disclosed to a partner with a clear and existing mandate to collect that information. In addition to publishing information about recipients' national security jurisdiction, for greater transparency, the core national security concept ("activities that undermine the security of Canada") would be streamlined to only include examples that would, in all cases, be activities that would undermine the security of Canada. As well, it would be clarified that advocacy protest, dissent, and artistic expression activities are not covered unless they are, or are carried out in connection with, national security threats. Further, amendments would be made to the disclosure threshold to clarify, among other things, the link that must exist between the information and the recipient's national security jurisdiction and responsibilities.

Disclosure Threshold

The Committee and other commentators have also raised concerns with respect to the threshold for disclosure of information. Currently the Act allows information to be disclosed if it is "relevant" to an activity that undermines the national security of Canada, which some consider to be low. Some have asked that the threshold be raised to "necessary" or that a dual threshold be established whereby "relevant" would be the threshold for disclosure and "necessary" would be the threshold for receiving information.

The Government has examined a variety of options in this regard. The key issue regarding the threshold is the need to establish specific decision making parameters for the discloser of information that will protect individual privacy but not cause undue delays in the information sharing process. To this end, the threshold would be clarified to set out specific requirements for the disclosure that would speak to the:

- utility of the information (it must contribute to the carrying out of the recipient's national security jurisdiction or responsibilities);
- integrity of the information (information on reliability and accuracy must be provided); and,
- privacy interests (disclosure may not affect any person's privacy interest more than is reasonably necessary in the circumstances).

In summary, the Government believes this approach would improve upon the previous "relevant" threshold as it would clarify the specific requirements for disclosure.

Accountability, Oversight and Transparency in the Information Sharing Process

(Pertaining to Recommendations 7 & 12-14)

The Committee echoes a number of the concerns raised by stakeholders, including the Privacy Commissioner of Canada, with respect to the need for increased accountability and transparency in the information disclosure process. The Government agrees that Canada's national security framework needs to be updated and will move forward an ambitious agenda in this regard. An important first step was the introduction of Bill C-22, *An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Act.* However, the Government understands that there is still more work to be done and is committed to working on addressing the remaining gaps in the accountability and transparency issues raised in the national security system.

The Government proposes to support all federal departments and agencies in their national security information disclosing capacity building by establishing a Centre of Expertise for information disclosure within the national security community. The Centre would have a specific mandate to provide leadership and guidance on information disclosing authorities and best practices, which would be consistent with the Privacy Commissioner's recommendation in his 2015-2016 Annual Report that more guidance and direction be provided to federal institutions as it pertains to aspects of the information disclosure process.

The Government would also introduce a new requirement that institutions maintain records with respect to all disclosures made under the Act and would specify what those records must contain. In addition, disclosing institutions would be required to provide these records to the National Security and Intelligence Review Agency (to be established). The Government is also committed to working with the Privacy Commissioner to address other accountability-related recommendations (such as those pertaining to Information Sharing Agreements and Privacy Impact Assessments).

Finally, to assist with the general understanding, intent and purpose of the legislation, the Government is proposing that the SCISA be re-named as "*The Security of Canada Information Disclosure Act*". The aim of this amendment would be to clarify that the scope of the legislation is limited to disclosures, which would help address concerns that the SCISA amends and/or broadens the collection authorities currently established for individual designated recipient institutions.

The Government believes that these amendments and non-legislative measures would increase transparency by clarifying how the SCISA will operate in conjunction with existing legal and policy frameworks and would assist government institutions in applying the Act to achieve the government's goal of encouraging and enhancing responsible information disclosure for national security purposes. On behalf of the Government, we would like to thank the Standing Committee on Access to Information, Privacy and Ethics for its comprehensive report. It will be a valuable resource as the Government moves forward with its commitment to enhance Canada's national security framework.

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

Mr. Blaine Calkins, M.P.
Chair
Standing Committee on Access to Information, Privacy and Ethics
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Calkins,

Pursuant to Standing Order 109 of the House of Commons and on behalf of the Government of Canada, we are pleased to respond to the report by the Standing Committee on Access to Information, Privacy and Ethics, entitled, *Safeguarding Canada's National Security while Protecting Canadians' Privacy Rights: Review of the Security of Canada Information Sharing Act (SCISA).*

We would first like to thank the Committee for undertaking this review of such an important piece of legislation in Canada's national security framework. In addition, we would like to express our appreciation to the experts who appeared before the Committee to provide their views and share their experiences in using the SCISA. The report by the Committee provides thoughtful and constructive recommendations to improve Canada's information sharing for national security purposes.

It is well known that national security institutions require information to detect, analyze, investigate and prevent threats and often times this requires multiple pieces of information from multiple different sources. Given today's national security environment, threats can evolve rapidly, therefore the appropriate tools need to be in place to ensure the timely and effective disclosure of information. The Air India Commission of Inquiry, the Auditor General and other commentators identified real and perceived barriers that were preventing Government officials from disclosing information for national security purposes. As such, the SCISA was created to provide a clear, explicit authority for Government of Canada institutions to disclose information for national security purposes. In particular, it provides a lawful authority for Government of Canada institutions to proactively disclose national security-relevant information to federal institutions with a national security jurisdiction or responsibilities and sends a clear signal that information may be disclosed to address national security threats.

The Committee's Report, the 2016 Consultation on National Security, and the Office of the Privacy Commissioner 2015-2016 Annual Report to Parliament have helped clarify for Canadians the purpose and scope of the Act. However, more work is needed to explain the SCISA's role in protecting our national security and its existing safeguards to protect privacy.

Moreover, the Government agrees with the Committee that changes are needed to improve the SCISA, particularly regarding clarifying its scope and requirements for disclosing information, as well as the need for greater direction and guidance on its use.

To this end, please find below the Government Response to the Parliamentary Committee's Report, organized along key themes identified through the recommendations:

Increased Transparency of the List of Designated Recipient Institutions

(Pertaining to Recommendations 1 & 2)

Schedule 3 of the SCISA currently allows 17 departments/agencies to receive information for national security purposes. Concerns have been raised as to why there are so many institutions included in the Act. The Government agrees with the Committee and the feedback received through the Consultation that a better explanation of the rationale for inclusion of each designated recipient institution is required. In response to these concerns:

- Deputy Heads would be asked to re-validate their institutions need to be a listed entity in Schedule 3, with the aim of ensuring that only institutions with clear national security jurisdiction or responsibilities will be included on the list;

- The Government would publish an overview of the national security jurisdiction and responsibilities of each recipient institution; and,

- We would make public which positions and/or directorates within the institution have been delegated by the Head of each institution to receive information, to further clarify that only areas dealing with national security matters, specifically institutions whose core mandate is not national security but which have national security responsibilities, are able to receive information under the SCISA.

Scope, Disclosure Threshold and Existing Information Management Authorities

(Pertaining to Recommendations 3-6 & 8-11)

Scope

The Committee expressed concern that the scope of the SCISA (i.e., the definition of "activity that undermines the security of Canada) is too broad. As such, stakeholders have asked for a narrowing of the definition or that the SCISA's definition be replaced by the definition found in the *CSIS Act* ("threats to the security of Canada"), which more clearly articulates which activities threaten Canada and is a more familiar and tested definition. The list of illustrative examples included in the SCISA has also raised questions about how the definition was to be applied, with some believing information collection authorities are expanded. And, finally, there were concerns that the Act could inhibit advocacy, protest, dissent and artistic expression.

To have value, the SCISA must cover all information that is needed for government institutions to carry out their national security responsibilities. These can range in scope from the Canada Border Services Agency's responsibility to provide integrated border services that support national security and public safety priorities to the Canadian Food Inspection Agency's responsibility to respond rapidly and effectively to food safety emergencies or threats to agricultural or forest biosecurity, including bioterrorism and agro-terrorism. An overly narrow scope could prevent important information from being disclosed to a partner with a clear and existing mandate to collect that information. In addition to publishing information about recipients' national security jurisdiction, for greater transparency, the core national security concept ("activities that undermine the security of Canada") would be streamlined to only include examples that would, in all cases, be activities that would undermine the security of Canada. As well, it would be clarified that advocacy protest, dissent, and artistic expression activities are not covered unless they are, or are carried out in connection with, national security threats. Further, amendments would be made to the disclosure threshold to clarify, among other things, the link that must exist between the information and the recipient's national security jurisdiction and responsibilities.

Disclosure Threshold

The Committee and other commentators have also raised concerns with respect to the threshold for disclosure of information. Currently the Act allows information to be disclosed if it is "relevant" to an activity that undermines the national security of Canada, which some consider to be low. Some have asked that the threshold be raised to "necessary" or that a dual threshold be established whereby "relevant" would be the threshold for disclosure and "necessary" would be the threshold for receiving information.

The Government has examined a variety of options in this regard. The key issue regarding the threshold is the need to establish specific decision making parameters for the discloser of information that will protect individual privacy but not cause undue delays in the information sharing process. To this end, the threshold would be clarified to set out specific requirements for the disclosure that would speak to the:

- utility of the information (it must contribute to the carrying out of the recipient's national security jurisdiction or responsibilities);
- integrity of the information (information on reliability and accuracy must be provided); and,
- privacy interests (disclosure may not affect any person's privacy interest more than is reasonably necessary in the circumstances).

In summary, the Government believes this approach would improve upon the previous "relevant" threshold as it would clarify the specific requirements for disclosure.

Accountability, Oversight and Transparency in the Information Sharing Process

(Pertaining to Recommendations 7 & 12-14)

The Committee echoes a number of the concerns raised by stakeholders, including the Privacy Commissioner of Canada, with respect to the need for increased accountability and transparency in the information disclosure process. The Government agrees that Canada's national security framework needs to be updated and will move forward an ambitious agenda in this regard. An important first step was the introduction of Bill C-22, *An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Act.* However, the Government understands that there is still more work to be done and is committed to working on addressing the remaining gaps in the accountability and transparency issues raised in the national security system.

The Government proposes to support all federal departments and agencies in their national security information disclosing capacity building by establishing a Centre of Expertise for information disclosure within the national security community. The Centre would have a specific mandate to provide leadership and guidance on information disclosing authorities and best practices, which would be consistent with the Privacy Commissioner's recommendation in his 2015-2016 Annual Report that more guidance and direction be provided to federal institutions as it pertains to aspects of the information disclosure process.

The Government would also introduce a new requirement that institutions maintain records with respect to all disclosures made under the Act and would specify what those records must contain. In addition, disclosing institutions would be required to provide these records to the National Security and Intelligence Review Agency (to be established). The Government is also committed to working with the Privacy Commissioner to address other accountability-related recommendations (such as those pertaining to Information Sharing Agreements and Privacy Impact Assessments).

Finally, to assist with the general understanding, intent and purpose of the legislation, the Government is proposing that the SCISA be re-named as "*The Security of Canada Information Disclosure Act*". The aim of this amendment would be to clarify that the scope of the legislation is limited to disclosures, which would help address concerns that the SCISA amends and/or broadens the collection authorities currently established for individual designated recipient institutions.

The Government believes that these amendments and non-legislative measures would increase transparency by clarifying how the SCISA will operate in conjunction with existing legal and policy frameworks and would assist government institutions in applying the Act to achieve the government's goal of encouraging and enhancing responsible information disclosure for national security purposes. On behalf of the Government, we would like to thank the Standing Committee on Access to Information, Privacy and Ethics for its comprehensive report. It will be a valuable resource as the Government moves forward with its commitment to enhance Canada's national security framework.

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