Minister of Public Safety,
Democratic Institutions
and Intergovernmental Affairs

Ministre de la Sécurité publique,
des Institutions démocratiques
et des Affaires intergouvernementales

Ottawa, Canada K1A 0P8

John Brassard, MP
Chair of the Standing Committee on Access to Information, Privacy, and Ethics
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Brassard,

As the Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs, and on behalf of the Government of Canada, I am pleased to respond to the tenth report of the Standing Committee on Access to Information, Privacy, and Ethics entitled, Foreign Interference and the Threats to the Integrity of Democratic Institutions, Intellectual Property and the Canadian State.

I would like to commend the Committee for its efforts to examine foreign interference in Canada. Foreign interference poses one of the greatest threats to Canada's national security, our way of life, and our economic prosperity and sovereignty. The Government agrees in principle with both the overall tenor and with a majority of the Committee's recommendations. While the Government does not disagree with any of the recommendations, further study or examination is required in some cases.

The Government is committed to addressing the foreign interference threat by modernizing Canada's policy and legislative framework in ways that align with our national values, respect Canadian rights and freedoms, and account for a wide range of perspectives and experience. The Government has already taken several steps to adapt Canada's toolkit to counter foreign interference in a way that emphasizes transparency and citizen engagement. For example, on May 9, 2023, public consultations on the development of a Foreign Influence Transparency Registry concluded. The Government of Canada also launched public consultations on November 24, 2023 about possible amendments to the Canadian Security Intelligence Service Act, the Criminal Code, the Security of Information Act, and the Canada Evidence Act to enhance the Government's ability to address foreign interference threats.

These initiatives, alongside the Government of Canada's other commitments to address the threat of foreign interference, are referenced in the enclosed Government Response to the Committee's 22 recommendations.

Once again, on behalf of the Government of Canada, I would like to thank the members of the Standing Committee on Access to Information, Privacy, and Ethics for the diligence and commitment undertaken in your work.

Sincerely,

The Honourable Dominic LeBlanc, P.C., K.C., M.P.
Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs

Recommendation 1: That the Government of Canada improve the declassification system for historical records, as recommended in its report on the state of the access to information system published in June 2023, and establish and implement clearer classification guidelines for national security records

The Government agrees with this recommendation.

The Government recognizes that the declassification of historical records, including national security archival records, is a vital component of government transparency. Transparency is fundamental to enabling national security and countering foreign interference (FI) by promoting Canadians' trust in democratic institutions.

The Government has an existing model to categorize information as set out in the Standard on Security Categorization in the Directive on Security Management. The security categorization process considers exemption and exclusion criteria of the Access to Information Act and the Privacy Act to ensure that resources are not applied to protect information that can be made public.

To further promote the declassification and downgrading of records within institutions, in December of 2023, the Government published an Implementation Notice on Leveraging Access to Information to Promote Declassification and Downgrading of Government Records. The notice provides guidance to government institutions on how they can leverage existing access to information (ATI) processes and training to initiate departmental procedures for declassifying or downgrading the security categorization of government records. The ability to declassify records consistently across the Government of Canada will reduce the burden on the ATI system and provide clarity to departments on actions to be taken.

Furthermore, the national security and intelligence community, Library and Archives Canada, Treasury Board of Canada Secretariat, the Department of Justice and Public Safety Canada are collaborating on a number of declassification initiatives focused on systematically declassifying historical records in general, and national security records in particular. These initiatives include:

- The establishment of an ad-hoc Interdepartmental Declassification Working Group, which provides advice on the systematic and proactive declassification of historical national security and intelligence records, and to inform declassification policy work across the Government of Canada; and
- The development of a draft national security and intelligence declassification framework that aims to set out a consistent and systematic approach to declassifying historical records, based on

existing best practices and the advice of the above-mentioned working group.

Recommendation 2: That the Government of Canada amend the Access to Information Act to clarify that the access to information system is based on a culture of openness and transparency, and that it implement the other recommendations of the Committee in its report on the state of the access to information system published in June 2023

The Government takes note of this recommendation.

The Government notes that in September of 2023, it provided a comprehensive response to the ETHI report on the state of Canada's access to information system. Work is underway to implement a range of actions to address the recommendations in that report, including several related to improving openness and transparency.

Recommendation 3: That the Government of Canada direct increased and regular sharing of relevant information to the public by the Canadian Security Intelligence Service in order to increase national security literacy

The Government agrees with this recommendation.

The Canadian Security Intelligence Service (CSIS) is committed to engaging and educating Canadians on national security issues. Given the rise in threats facing Canada, CSIS has made significant efforts to increase outreach and awareness of threats, and will continue to do so. This includes targeted engagement with community groups and associations, private industry, academic and research institutions, and municipal and indigenous organizations, as well as general awareness engagement with the public at large.

However, CSIS currently faces limitations on sharing classified information outside the Government of Canada. Such limitations prevent CSIS from directly sharing information that could help domestic partners, such as the private sector and academic institutions, build resilience to FI and espionage threats. This is why the Government is consulting Canadians on potential amendments to the CSIS Act that would authorize CSIS to disclose information to other entities or persons, in addition to the Government of Canada, on threats to the security of Canada, for the purpose of increasing awareness and resiliency.

Notwithstanding this, to safeguard its ability to investigate and advise on threats, CSIS has a responsibility to protect its sources and methodologies. Therefore, while CSIS is committed to sharing information with the public wherever possible, and has taken steps to increase this in recent years

through speeches and other events, there will always be limitations on the information that can be disclosed.

Together with the Federal government, provincial, municipal, and indigenous governments; private industry academia; community groups; and Canadians in general all have a role to play in increasing societal national security literacy and resilience. The Government of Canada is eager to expand partnerships as part of these efforts.

Recommendation 4: That the Government of Canada strengthen rules and penalties governing illicit disclosure of national security intelligence

The Government takes note of this recommendation.

The Security of Information Act (SOIA) is central in countering espionage in Canada. Subsection 4(1)(a) of the SOIA ("unlawful disclosure") makes it an offence to communicate unlawfully, secret or official information to persons not authorized to receive the information. The companion subsections 4(3) ("receipt") and 4(4)(b) ("allowing possession") create offences for unlawfully receiving secret information and for transmitting secret information to someone not authorized to receive it.

In 2006, Subsections 4(1)(a), 4(3) and 4(4)(b) were successfully challenged in the Superior Court of Ontario as being contrary to sections 2(b) (freedom of expression) and 7 (life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice) of the Charter. However, the regime in sections 8 to 15 of the Security of Information Act remains, and has been relied upon to bring about convictions for unlawful disclosure of special operational information.

The Government is currently assessing whether it is desirable and appropriate to make amendments to the SOIA. It is seeking Canadian input on the issue through public consultations on potential legislative changes aimed to address the threat of FI, as discussed in the response to Recommendation 5.

Recommendation 5: That the Government of Canada ensure that any legislative mechanisms developed to counter foreign interference take into account how they might affect individuals and communities already victimized or targeted by foreign interference in Canada, and that it include these communities in developing measures to counter the impacts of interference on them

The Government agrees with the recommendation.

Understanding how different groups may be uniquely or disproportionately affected by FI is critical to the Government's efforts to countering this threat.

In an effort to promote transparency and build trust, Public Safety Canada held in-person and online consultations on a potential Foreign Influence Transparency Registry (FITR) for Canada in the spring of 2023.

The purpose of the consultations was to solicit feedback from the Canadian public and stakeholders on how Canada might design and implement a FITR to strengthen national security by increasing transparency and general public awareness of FI in Canada. Information was received from over 1,000 online respondents and over 80 key stakeholder groups.

On November 24, 2023, the Government launched additional public consultations on potential legislative amendments to help address FI. The Government has since held a series of roundtable discussions with communities affected by FI activities to seek their views on potential legislative mechanisms. The participants included members of the Cross-Cultural Roundtable on Security and representatives of people in Canada who have been targeted by foreign states for their advocacy.

Potential amendments mentioned in the public consultations include changes to the Canadian Security Intelligence Service Act that would allow CSIS to share information with non-federal stakeholders. A greater ability to share information would help these stakeholders improve their resilience to FI. Other proposed amendments include strengthening laws against foreign-influenced threats of violence against individuals, and new offences to protect democratic processes at all levels of government against FI.

Feedback provided by community groups, individuals, and others will help inform the design of any potential legislative amendments to counter FI that may be introduced in Parliament.

Recommendation 6: That the Government of Canada review and update Canada's national security policy, and that the new policy outlines the rules allowing the Canadian Security Intelligence Service to directly warn federal Members of Parliament of threats related to foreign interference

The Government takes note of this recommendation.

The Government is continuously evaluating and adapting Canada's national security policy framework. Currently, the Canadian Security Intelligence Service Act limits CSIS' authority to disclose information, except in limited situations. To work within these limitations, CSIS provides high-level, unclassified, and general threat briefings to those targeted by foreign inference. For example, in 2021, CSIS provided 45 briefings to Parliamentarians, comprised of 2 Senators and 43 Members of Parliament. In 2022, CSIS provided 49 briefings with federal elected officials. CSIS continues to provide briefings to officials as necessary, and any threat to personal safety will always be immediately referred to law enforcement. In

the April 6, 2023, report "Countering an evolving threat: Update on recommendations to counter FI in Canada's democratic institutions," the Government committed to making new unclassified briefings available to Parliamentarians and their staff, and to providing briefings to Parliamentarians upon their swearing-in and on a regular basis thereafter. In May 2023, the Minister of Public Safety issued a Ministerial Direction stating that threats to the security of Canada directed at Parliament and Parliamentarians will continue to receive the highest level of attention from CSIS.

The Integrated Terrorism Assessment Centre (ITAC), which was established as part of Canada's 2004 National Security Policy, and which operates under the authorities of the CSIS Act, has also responded to the need for threat assessments that are broader than its traditional focus on violent extremism. ITAC has published 13 all-threat assessments (ATAs) pertaining to threats against federal public officials and has provided four briefings to the subjects of ATAs. These assessments include, but are not limited to FI.

The Government will seek to ensure that potential review or updates to the national security policy framework, including policies pertaining to CSIS, address evolving threats such as FI.

Recommendation 7: That the Government of Canada make full use of existing legislation, such as the Security of Information Act and other relevant Acts as enforcement resources and tools

The Government of Canada agrees with this recommendation.

The Government makes full use of its legislative toolkit to tackle the various types of FI against Canada. Investigative and enforcement agencies can leverage legislation such as the Security of Information Act (SOIA), the Security Offences Act (SOA), and the Criminal Code to investigate FI-related criminality. For instance, SOIA contains numerous offences in relation to FI, which allow for the criminal prosecution of those complicit in economic espionage, the release of classified information, foreign influence threats and violence. Likewise, the Criminal Code contains offences that support the investigation, prosecution, and punishment of FI actors and their proxies, including breach of trust, criminal harassment, unauthorized use of a computer, intimidation, and bribery. The RCMP investigates FI related criminal activity and works with the Public Prosecution Service of Canada to lay charges where appropriate. Charges were brought for the first time under the economic espionage offence in November 2022.

Even when the criminal prosecution of FI actors is not viable, the full use of other legislative tools by the Government of Canada allows for the disruption of FI-related activities that would, otherwise, take place. For instance, the Investment Canada Act provides a national security review process that

allows the government to review foreign investments to ensure they are not harmful to Canada's national security, which includes factors such as ensuring that investments cannot be used to promote the strategic objectives of foreign states to the detriment of Canada's security and economic prosperity. In a similar fashion, the Canadian Passport Order allows the Government of Canada to cancel or revoke a passport belonging to a person believed to be engaging in FI-related activities.

Recommendation 8: That the Government of Canada update its national security policy to include a policy on the threats caused by the use of artificial intelligence by foreign actors

The Government will examine this recommendation further.

The Government of Canada is positioning itself to ensure that it is prepared for and able to address the evolving threats caused by the use of AI by foreign actors through a variety of initiatives.

For example, Public Safety Canada's Research Security Centre reviews grant applications, including those involving AI, under the National Security Guidelines for Research Partnerships; producing and delivering advice on protecting research; and, delivering tailored advice to research institutions based on their specific needs. Additionally, the Communications Security Establishment, Global Affairs Canada, Justice Canada, the Royal Canadian Mounted Police, and the Canadian Security Intelligence Service, all have ongoing initiatives to effectively research and establish guidelines for the responsible use of AI within their respective organizations.

Public Safety Canada also leads the development of an updated National Cyber Security Strategy (Strategy) in collaboration with the federal cyber security community. As AI evolves, it is important to consider its current and potential nexuses with national cyber security. The new Strategy would articulate Canada's long-term approach to protect its national security and economy, deter cyber threat actors, and promote norms-based international behaviour in cyberspace.

Recommendation 9: That the Government of Canada invest in Canada's strategic digital literacy and capabilities and those of its national security agencies to improve the ability to detect and counter foreign interference activities conducted with artificial intelligence

The Government agrees with this recommendation.

The Government of Canada will continue to remain aware of, continually assess, and respond to evolving threats, including from new technologies such as artificial intelligence (AI), which can accelerate or amplify FI activities.

The Government is investing in programs and conducting awareness campaigns to increase digital literacy in Canada to address cyber threats and disinformation from various fronts. As Canada's technical authority for cyber security, CSE's Canadian Centre for Cyber Security (CCCS) conducts awareness campaigns like Get Cyber Safe and releases regular threat assessments and guidance documents to educate Canadians about the range of cyber threats they face, such as those from AI. CSE's guidance includes the National Cyber Threat Assessment, Cyber Threats to Canada's Democratic Processes, Guidance on Generative AI, and CSE's Annual Report; as well as regular alerts and advisories.

Canadian Heritage has also invested over $21 million since 2019 to support digital media and civic literacy activities in Canada through the Digital Citizen Contribution Program (DCCP). The DCCP helps fund projects run by researchers and civil society organizations to better understand and build resilience to online disinformation, including disinformation related to FI. The DCCP's latest call for proposals is to support projects that develop and publish tools to help people in Canada identify content created and spread by bots and/or artificial intelligence, and to build resilience to mis-/disinformation stemming from foreign governments targeting people in Canada, including diaspora communities.

To help foster home-grown Canadian AI capabilities, CSE also invests in technical skills and supports research and development into AI. For example, CSE and the Natural Sciences and Engineering Research Council of Canada have partnered to fund research communities to conduct research on robust, secure, and safe AI. In addition to contributing to the body of AI knowledge, this funding will help produce a new generation of data scientists and engineers who are sensitive to the issues around robust, secure, and safe AI. CSE further supports AI training needed for Government of Canada employees to build the necessary skills to harness the capacity of AI and be able to safeguard against potential risks all the while building trust in the deployment of AI technologies within organizational contexts. All these efforts contribute to raising Canada's cyber security capabilities.

Recommendation 10: That the Government of Canada ensure that the Canadian Security Intelligence Service provide more training and information to Canadian parliamentarians and public servants on the threats posed by foreign interference in Canada, the various tactics used by foreign actors and the means to counter them

The Government agrees with this recommendation.

While operating within the bounds of its current governing legislation, the Canadian Security Intelligence Service (CSIS) provides parliamentarians with as many details as possible to mitigate the threat of FI. For example, in 2021, CSIS provided 45 briefings to two Senators and 43 Members of

Parliament. In 2022, CSIS provided 49 briefings to federal elected officials. CSIS will continue to provide briefings to officials as necessary and any threat to personal safety will always be immediately referred to law enforcement.

Other Government of Canada departments are also involved in ensuring Parliamentarians are aware of the threat of FI, as countering FI is a whole-of-society effort. For example, as part of the Plan to Protect Canada's Democracy, political parties recognized in the House of Commons are able to nominate key personnel to receive security clearances to permit them to receive classified briefings during the election period. In the April 6, 2023, report "Countering an evolving threat: Update on recommendations to counter FI in Canada's democratic institutions," the Government committed to making new unclassified briefings available to Parliamentarians and their staff, and to providing briefings to Parliamentarians upon their swearing-in and on a regular basis thereafter. The Government also committed to implementing a counter disinformation toolkit and offering training for Parliamentarians on FI and disinformation. Work to deliver these commitments is ongoing. Government agencies such as the Communications Security Establishment, Global Affairs Canada, the Canada School of Public Service, and Treasury Board Secretariat, have all since worked to develop and disseminate knowledge to parliamentarians on FI.

Recommendation 11: That the Government of Canada establish a foreign interference awareness program for use by academic and research institutions

The Government agrees with this recommendation.

In Budget 2022, Public Safety Canada received funding to establish the Research Security Centre, which is responsible for providing research security-related outreach to academic institutions, provinces, and researchers across the country. Through a network of six regional advisors located across the country, the Research Security Centre disseminates advice, conducts research security workshops, and aids external stakeholders in accessing Government of Canada services and information. Part of these outreach initiatives include the Safeguarding Science program which offers workshops to the Canadian research and academic community and provides a broad overview of research security threats and mitigation measures.

This work is complemented by the Canadian Security Intelligence Service's (CSIS) Academic Outreach and Stakeholder Engagement program. The program aims to share information as widely as possible, within security and legislative restrictions. For example, CSIS routinely provides security briefings and mitigation strategies to university officials and faculty on the threat environment. CSIS has briefed more than 200 organizations and 1,000 individuals on the possible threats, and tools to protect themselves, their

research and their employees. CSIS also has regular bilateral engagements with over 70 universities, colleges, and university and college associations. This enables stakeholders, including the academic community, to work in partnership with the Government of Canada and build resilience against threat-related activity, including FI on campus.

Innovation, Science and Economic Development (ISED) leads the Government of Canada-Universities Working Group, which is comprised of several Government of Canada partners as well as Canadian research institutions and serves as a table for consultations on research security policies. ISED also maintains the Safeguarding Your Research portal which is regularly updated and includes useful information, advice, and online training courses on how to best safeguard research and intellectual property. Budget 2022 also included $25 million ongoing for the Research Support Fund to build research security capacity within post-secondary institutions to identify, assess and mitigate potential risks to research security.

In addition to other ongoing efforts to ensure that key stakeholders are made aware of threats to research security, the Communications Security Establishment (CSE) and its Canadian Centre for Cyber Security (CCCS) serve as the single unified source of expert advice and guidance, services and support on cyber security for Canadians and Canadian organizations, including higher education institutions. The Royal Canadian Mounted Police, through the Federal Policing Strategic Engagement and Awareness (FP-SEA) also participates in outreach activities with the academic sector. FP-SEA engages with stakeholders including academia in distributing publications and holding in-person operational information sessions on Federal Policing priority enforcement areas including FI.

Recommendation 12: That the Government of Canada, in collaboration with national security agencies, establish rigorous mechanisms to ensure that any contractual arrangements between Canada and foreign suppliers do not create high risk to national security

The Government will examine this recommendation further.

The Government recognizes the importance of mitigating national security threats in the procurement of goods and services and has mechanisms in place to identify and address risks. For example, security requirements are identified through the completion of a Security Requirements Checklist (SRCL), which then determine which security clauses to include in contracts.

The Government also seeks bilateral security arrangements with partner foreign governments to ensure the reciprocal sharing of information on foreign suppliers. Based on this, the Communication Security Establishment (CSE) conducts Supply Chain Integrity (SCI) assessments for the

procurement of Information Communication Technologies (ICT) used by the Government of Canada. These assessments identify supply chain threats, risks, and vulnerabilities, and include a Foreign Ownership, Control or Influence assessment to mitigate the risk of foreign influence on government classified information and assets. The SCI program is expanding to address digital supply chain risks in critical infrastructure, in support of Bill C-26.

The Canadian Security Intelligence Service (CSIS) also prioritizes investigating potential hostile economic activities by state actors. CSIS supports Government of Canada partners in their risk management practices related to the Foreign Ownership, Control or Influence and Controlled Goods programs. CSIS also works closely with government partners to ensure that as many Canadian businesses and different levels of government as possible are aware of the threat environment and that they have the information they need to implement pre-emptive security measures. CSIS's outreach to Supply Chain Canada and other related industry groups on logistics supply network risks is one example of how CSIS is engaging with a wide variety of stakeholders to ensure Canadians remain safe and Canadian interests are protected from threats.

To respond to evolving national security risks, the Government is exploring the development of rigorous tools and processes to address national security risks specifically. Public Services and Procurement Canada has established a working group that will engage with Canada's national security agencies, including CSE, on the potential development of a Security Pre-Assessment Risk Questionnaire (Screening Tool). The Screening Tool would be used at the pre-solicitation phase to identify requirements that pose a high, medium, or low national security risk. Based on the level of risk identified, mitigation measures would be incorporated into the procurement strategy, such as a broadened SCI assessment that would apply to more commodities with ICT components. In conjunction with existing ones, this new tool would allow for a more robust response to national security threats.

Recommendation 13: That the Government of Canada work with minority-language communities affected by foreign interference activities in Canada to provide them reliable information on the Canadian democratic process, including information on government policies and programs that may affect them, in the language they understand best, and that the government engage with local and ethnic medias to provide that information

The Government will examine this recommendation further.

The Government of Canada is committed to ensuring information about Canada's democratic institutions and the Government of Canada's policies and programs reaches all Canadians. The Government of Canada provides information on Canada's democratic institutions, how Parliament works, basic

information about how to vote, and how Canadians are represented online on Canada.ca. This information is provided in English and French, as per the Official Languages Act. The Government of Canada will examine the possibility of translating resources about Canada's democratic institutions into other languages spoken in Canada, including by working with minority language communities.

In 2018, the Elections Modernization Act expanded Elections Canada's mandate to communicate with the public to make the electoral process better known. Elections Canada's mandate includes conducting public information campaigns on voter registration, voting and becoming a candidate. According to Elections Canada's Report on the 44th General Election of September 20, 2021, the agency's "Guide to the Federal Election" booklet was translated to 49 different languages, including 16 Indigenous languages. The Government of Canada welcomes Elections Canada's initiatives to ensure all Canadians have reliable information about the voting process.

Several Government agencies, including the Canadian Security Intelligence Service (CSIS), Global Affairs Canada (GAC), and Canadian Heritage, dedicate considerable efforts to engage with the public, including through the development of publicly available resources. CSIS has reported on FI in all its annual public reports for the last 30 years, and has published unclassified reports, including 'Foreign Interference and You', in six languages, to reach as many Canadians as possible. CSIS' products are published in a range of foreign languages to ensure that vulnerable communities can access threat information in their language of choice.

When appropriate, GAC distributes public statements on FI and engages with affected individuals from minority-language communities in the language they understand best. In August and October 2023, GAC released public statements in both official languages and distributed them to a list of media contacts in Mandarin, following two separate campaigns where GAC deemed it likely that the People's Republic of China (PRC) was involved in targeting Canadian Parliamentarians. The first campaign targeted a Member of Parliament on WeChat, while the second campaign targeted over 40 Parliamentarians and a dissident of Chinese descent living in Canada across social media platforms.

Canadian Heritage has invested over $21 million since 2019 to support digital media and civic literacy activities in Canada through the Digital Citizen Contribution Program (DCCP). The DCCP provides time-limited financial assistance to projects run by researchers and civil society organizations to better understand and build resilience to online disinformation, including disinformation related to FI, and to support Canada's democracy. Many of the projects supported though the DCCP have specifically aimed to equip minority language communities with tools to build resilience to online

disinformation. The DCCP's Fall 2023 call for proposals seeks out projects to develop and publish tools to build resilience to mis-/disinformation stemming from foreign governments, such as the PRC and Russia, targeting people in Canada, including diaspora communities, among other priorities.

Recommendation 14: That the Government of Canada include in the Criminal Code criminal penalties that cover all foreign interference operations, including harassment and intimidation by a foreign state, and that it provide appropriate sanctions

The Government agrees in principle with this recommendation.

The Government launched public consultations on potential amendments to the Canadian Security Intelligence Service Act (CSIS Act), the Criminal Code, the Security of Information Act (SOIA) and the Canadian Evidence Act (CEA) on November 24, 2023 as part of its counter FI efforts.

The Department of Justice Public Consultation Paper outlines several proposals to amend SOIA, including:

- creating new FI offences, including a general FI offence, to better address FI risks to Canada, as well as transnational repression of people living in Canada and their families abroad, and to ensure that covert hostile activities are fully addressed by the criminal law;
- expanding the preparatory acts offence (s. 22), which targets doing anything in preparation of the commission of an offence, to cover all SOIA offences, and enhancing the existing penalties.

Proposed amendments to the Criminal Code include modernizing the sabotage offence by clarifying the types of critical infrastructure that could be targeted by sabotage. Additionally, creating an offence of sabotage for the benefit of a foreign state, is also under consideration.

Recommendation 15: That the Government of Canada clarify the purpose of the provisions of the Security of Information Act to counter foreign interference operations and its related sanctions, and that it implement a policy enabling Canadians to better understand how the Security of Information Act protects Canada from foreign interference

The Government agrees in principle with this recommendation.

As part of the Government of Canada's efforts to counter FI, on November 24, 2023, public consultations on potential amendments to the Canadian Security Intelligence Service Act, the Criminal Code, the Security of Information Act, and the Canada Evidence Act were announced.

The accompanying Department of Justice Public Consultation paper explains key provisions of the Security of Information Act that address aspects of transnational repression:

- Section 20 of the Security of Information Act, makes it an offence to induce, by threat, accusation, menace or violence, any person to do anything or to cause anything to be done, at the direction of, for the benefit of, or in association with a foreign state.

- Section 22 is a preparatory acts offence that makes it an offence to do anything that is specifically directed towards or specifically done in preparation of the commission of certain other Security of Information Act offences, including offences relating to FI.

Recommendation 16: That the Government of Canada hold online platforms accountable for publishing false or misleading information and that it develop policies to support the media ecosystem in communities and linguistic minority communities not represented by mainstream media to ensure that vulnerable communities are not revictimized

The Government takes note of this recommendation.

The Government is committed to introducing legislation as soon as possible to combat serious forms of harmful online content. To inform the development of this legislation, the Government has consulted widely through a public online consultation, an Expert Advisory Group, a Citizens' Assembly, and a series of 20 roundtables between July and November 2022.

Throughout these consultations, the Government heard that new legislation must strike a careful balance between ensuring a healthy and trustworthy online environment and protecting freedom of expression as guaranteed by Canada's Charter of Rights and Freedoms. Similarly, the Government heard from Canadians and stakeholders that while false and misleading information online can carry significant consequences, creating legislation and policies that restrict or otherwise limit speech based on the veracity of information would undermine freedom of expression to an unacceptable degree.

Fortunately, legislation is not the only tool in the Government's toolbox to combat false or misleading information. The Government is committed to addressing online disinformation and its effects on communities across the country. To this end, the Department of Canadian Heritage's Digital Citizen Initiative, established as part of the Plan to Protect Canada's Democracy, provides time-limited financial assistance to researchers and civil society organizations in Canada to explore the origins, spread, and impact of online disinformation and to build citizen resilience to it. Through its contributions

program, the Digital Citizen Contribution Program (DCCP), the DCI has invested $21 million in funding to support 109 projects, many of which support efforts to build resilience to disinformation in vulnerable communities.

In June 2023, the Government announced a $5.5 million investment into creating the Canadian Digital Media Research Network (CDMRN) which is independently administered by University of Toronto and McGill University. The CDMRN will further strengthen Canadians' information resilience by researching how the quality of information, including disinformation narratives, impact Canadians' attitudes and behaviours and by supporting strategies for Canadian digital literacy.

Recommendation 17: That the Government of Canada, in collaboration with national security agencies, explore the possibility of imposing targeted sanctions against Canadian companies that are exporting or selling technology to countries that use it to engage in foreign interference operations

The Government takes note of this recommendation and agrees that certain technologies can increase the reach and effectiveness of FI operations. Canada remains committed to playing a leadership role in the preservation and strengthening of an international rules-based order, and sanctions continue to be considered as part of this approach.

Canada has established a rigorous due diligence process to consider and evaluate circumstances that may warrant the use of sanctions. The Government also considers the broader political and international context when deciding whether sanctions or any other tools in Canada's foreign policy toolbox may be an appropriate response. Recommendations for sanctions are reviewed by Global Affairs Canada (GAC) through the prism of legislative requirements and available evidence to determine eligibility and suitability for sanctions under Canadian autonomous sanctions legislation, the Justice for Victims of Corrupt Foreign Officials Act (JVCFOA), and the Special Economic Measures Act (SEMA).

Due to the design, structure, and purpose of Canadian autonomous sanctions legislation, sanctions would not be an appropriate foreign policy tool to take action against Canadian companies that are exporting or selling technology to countries that use it to engage in FI operations. Under the JVCFOA, only individuals (i.e., not entities) can be listed, specifically for gross violations of human rights or significant acts of corruption.

The SEMA allows for the listing of entities. However, in order to be designated, an entity engaging in FI would need to fit the definition of "designated person", which stipulates that the person (i.e., individual or entity) must be in a foreign country, is or was a national of that foreign

country, and does not ordinarily reside in Canada. As such, Canadian companies are unable to be listed under SEMA. Designating or listing a Canadian company under SEMA regulations would create negative impacts on Canadians and Canadian businesses affiliated with the listed entity. Sanctions under SEMA impose a dealings ban (effectively an asset freeze), restrictions or prohibitions on trade, and restrictions on financial transactions or other economic activity. Therefore, it would be difficult for other Canadians to deal with a listed person in Canada, and this would have many practical implications. For example, any Canadian employee of a sanctioned Canadian company could not receive payment from their employer. Moreover, it is important to keep in mind that being sanctioned would be detrimental to a company's operations as all financial transactions would be barred (banks would cease facilitation and the company could not pay bills, etc.), eventually leading the company to bankruptcy.

Recommendation 18: That the Government of Canada establish a foreign influence registry as soon as possible

The Government agrees in principle with this recommendation.

Canada has a robust framework for transparency in lobbying, however, this framework was not designed to address threats from malign foreign influence, whereby some foreign governments use individuals or entities to attempt to influence covertly, or in a non-transparent manner, Canadian government policies or Canadian public discourse. For this reason, in March 2023, the Government of Canada launched public and stakeholder consultations on a Foreign Influence Transparency Registry (FITR). The online consultations lasted 60 days and produced nearly 1,000 responses from a wide range of respondents across Canada. This feedback is being examined by Public Safety Canada officials to guide the design of a FITR and associated legislation. Roundtable and bilateral discussions with stakeholders on a FITR, as well as on FI more broadly - including with community organizations, Indigenous groups and Provincial/Territorial stakeholders – are ongoing. The input from these consultations is informing decision-making and the design of new measures that could be brought forward.

Recommendation 19: That the Government of Canada amend the National Security and Intelligence Committee of Parliamentarians Act to require that each annual report tabled before each House of Parliament include a yearly review of foreign interference threats in Canada, such as harassment and intimidation of certain Canadian communities by foreign states

The Government takes note of this recommendation

The Government would like to highlight the existing review mandate of the National Security and Intelligence Committee of Parliamentarians (NSICOP).

The Committee has the ability to review: the legislative, regulatory, policy, administrative, and financial framework for national security and intelligence; any activity carried out by a department that is related to national security or intelligence unless the review would be injurious to national security; and any matter relating to national security or intelligence that a minister of the Crown refers to the Committee. The broad mandate provides NSICOP with discretion to review matters such as FI.

Several of NSICOP's reviews have already yielded recommendations regarding the Government of Canada's response to FI. For example, in March 2023, NSICOP completed a review to assess the state of FI in federal electoral processes. In 2018, NSICOP also published a special report examining FI in relation to the Prime Minister's visit to India in 2018. Additionally, in its 2019, 2021, and 2022 annual reports, NSICOP examined and put forth recommendations in relation to foreign inference. From these reports, between 2018 and 2023, a total of 26 recommendations were made to improve the government's response to FI, with significant work done to implement many of the recommendations, and continuing work being done on others.

Legislating specific requirements for the annual review could potentially impact the ability of NSICOP's reviews to evolve over time, as the threat landscape changes. The Government would like to emphasize the importance of maintaining NSICOP's independence and impartial nature as a review body, which is essential to maintaining the trust and confidence of Canadians.

Bill C-22 (An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts) created NSICOP in 2017 and requires that a comprehensive review of the provisions and operation of the Act be undertaken five years after coming into force. Recommendations, including those related to FI, could be further considered during a potential review of Bill C-22. The Act provides that the comprehensive review be undertaken by a committee of the House of Commons, of the Senate, or of both Houses of Parliament as designated or established by the House of Commons or the Senate, or by both Houses of Parliament, as the case may be.

Recommendation 20: That the Government of Canada create a Cabinet committee on national security

The Government agrees with this recommendation.

As announced by the Prime Minister on July 26, 2023, a new Cabinet committee on national security has been established. The National Security Council, which is chaired by the Prime Minister, serves as a forum for

strategic decision-making and for sharing analysis of intelligence in its strategic context.

Recommendation 21: That the Government of Canada strengthen reporting mechanisms for victims of harassment or intimidation by foreign entities, to ensure better coordination of the government response to such incidents and appropriate actions on individual complaints

The Government agrees with this recommendation.

The Government of Canada has various reporting mechanisms in place to report suspected incidents of FI and is making investments to help protect those targeted by FI and ensure a more coordinated federal response to these threats. At the federal level, the Royal Canadian Mounted Police (RCMP) investigates potential threats of violence, harassment and intimidation involving a state actor, and works with police of jurisdiction to detect and counter threats. The RCMP encourages community leaders to remain vigilant and report any suspicious activity to their local police or the RCMP. Individuals may contact the RCMP National Security Information network by phone at 1-800-420-5805 or by e-mail at RCMP.NSIN-RSIN@rcmp-grc.gc.ca. If someone in the public is in immediate danger, they should call 9-1-1 or contact their local police. In addition to existing mechanisms, Budget 2023 provided $48.9 million over three years for the RCMP to help further protect Canadians from harassment and intimidation by foreign actors, to increase its investigative capacity, and to more proactively engage with communities at greater risk of being targeted.

Additionally, the Canadian Security Intelligence Service (CSIS) has a general hotline and an online reporting mechanism on the Service's web page, where Canadians can report any concerns, including those related to FI. The hotline is 613-993-9620, toll-free at 1-800-267-7685. The TTY/TDD number is 613-991-9228. The online reporting mechanism is on CSIS' web page (www.canada.ca/security-intelligence-service) under "Reporting National Security Information". To protect the national security of Canadians, CSIS continues to invest significant effort in building relationships through its engagement with academia, business leaders, provincial, territorial, municipal, and indigenous governments, community leaders and members, and advocacy groups who may be targeted by threat actors. CSIS will engage different Canadian communities to gain unique insights and perspectives and also to provide important security information to potential targets of FI threats.

To enhance coordination within the federal government, in March 2023, the Prime Minister announced the creation of a Counter-FI Coordinator within Public Safety Canada. The role of the coordinator is to provide a dedicated focus on FI and enhance partnerships with non-federal stakeholders,

including raising awareness of the FI threat and tools available at the public's disposal to report these threats when observed. Budget 2023 has provided $13.5M over five years and $3.1M ongoing to this initiative.

While individuals may not be notified on updates or outcomes related to the threat reporting due to the sensitive nature of investigations, the Government of Canada takes these concerns seriously and values all information received through threat reporting. Above all else, the Government of Canada will continue to ensure the privacy and security of those who report these threats.

Recommendation 22: That the Government of Canada consult communities affected by foreign interference activities in Canada in any inquiry into foreign interference

The Government agrees with this recommendation.

On September 7, 2023, the Government announced the establishment of a Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, following extensive consultations with all recognized parties in the House of Commons. The inquiry is led by the Honourable Marie-Josée Hogue, puisne judge of the Quebec Court of Appeal, whose work as Commissioner began on September 18, 2023. Appointed under the Inquiries Act, the Commissioner operates independently from the government and has a full range of powers, including the power to compel witnesses and testimony on matters within federal jurisdiction. Commissioner Hogue is mandated to make any recommendations she deems appropriate to better protect Canada's democratic processes from FI, including in relation to the supports and protections for members of diaspora communities who may be especially vulnerable to FI in Canada's democratic processes.