Minister
of Public Safety
and Emergency Preparedness

Ministre
de la Sécurité publique
et de la Protection civile

Ottawa, Canada K1A 0P8

DEC 18 2020

Colleagues,

Foreign interference has recently been a topic of interest and discussion in the House of Commons.

In response to the motion that passed in the House on November 18th, 2020, I am writing to provide you with an overview of what the Government of Canada is doing to address these threats to the security, prosperity and democratic institutions of our country.

As we have adjourned for the winter break, I want to ensure you have something in writing before the session restarts in 2021.

I am happy to formally table the contents of this letter next month.

First-and-foremost, our Government does not, and will never, tolerate these types of activities.

Before I explain some of the ways in which the Government works to protect Canadians and counter these threats, I would like to emphasize that regarding this motion, particularly clause (b), the Government of Canada is always working to refine and further its plans to address foreign interference in Canada.

Work in this area has been longstanding and remains ongoing. This motion provides an opportunity to inform Canadians of what steps have been taken while assuring them that our agencies will always adapt to meet evolving threats.

We understand foreign interference to be hostile activity undertaken by foreign states that is purposely covert, malign, clandestine and deceptive. It can include threats, harassment and intimidation. These activities can be directed at Canadians, or residents of Canada, or against Canadian institutions to advance their strategic interests at the expense of our national interest and values. Hostile foreign states cross a line anytime they go beyond standard diplomacy to conduct activities against Canada that attempt to threaten our citizens, compromise our way of life, undermine our democratic processes, or damage our economic prosperity.

Canada

Modern foreign interference represents a complex threat. It poses a significant threat to the integrity of our political system, democratic institutions, social cohesion, academic freedom, economy and long-term prosperity as well as fundamental rights and freedoms. It can also affect the safety of our citizens and those who live here. This is not new. But it remains unacceptable as it targets all orders of government – federal, provincial and territorial, and municipal, as well as Canadian communities.

Foreign threat actors can use human intelligence operations, state-sponsored or foreign-influenced media, and sophisticated cyber tools, among others, to achieve their objectives. These include advancing their interests, sometimes at our expense, in an effort to achieve geopolitical influence, increase their economic advantages, access sensitive research, technology or information, revise the rules-based international order, enhance their domestic stability, and gain military advantage.

The 2019 Canadian Security Intelligence Service (CSIS) Public Report states that foreign interference activities are directed at Canadian entities both inside and outside of Canada, and directly threaten Canada's national security and strategic interests. Further, the Annual Report of the National Security and Intelligence Committee of Parliamentarians (NSICOP) outlined foreign interference activities, including the targeting of Canadian institutions and certain communities.

I will note that the Prime Minister took the important step of permitting the unclassified, publicly-released version of the NSICOP report to, for the first time, specifically name the People's Republic of China (PRC) and Russia as being particularly active in Canada. This was intended to raise public awareness of the threats posed by these countries. Additionally, the Canadian Centre for Cyber Security Report on National Cyber Threat Assessment 2020 also included reference to these countries as well as Iran and North Korea. Recently, the Standing Committee on Public Safety and National Security heard testimony from Mr. Scott Jones who declared that decisions about whether to list countries in these publications are not easy, but ultimately we need to acknowledge that these countries pose a risk while working to raise Canadians' awareness.

With an open and stable economy, skilled workforce, and advanced infrastructure, Canada is an attractive destination for foreign investors. The vast majority of foreign investment in Canada is conducted in an open and transparent manner and is beneficial to Canada's economy. However, the Government of Canada is increasingly concerned that certain types of investment transactions undertaken by foreign adversaries can harm national security. Foreign investments that give these entities control over, or access

to, sensitive technologies, critical infrastructure or the sensitive personal data of significant numbers of Canadians are of particular concern.

Certain governments, and their proxies, are prepared to use illicit means to obtain goods, sensitive information and technology. These proxies could include state-owned enterprises, individuals engaged with academic institutions and trade organizations, or other entities that are not directly linked to a state itself but may still serve its interests.

For example, talent programs are an acceptable part of the modern research enterprise, however some foreign threat actors can use them for malicious purposes. The requirement to transfer or replicate research, requirements to attribute research to foreign institutions, or to conceal affiliations to foreign military or intelligence services, are ways in which foreign actors, including the PRC, use talent programs to acquire sensitive technology and knowledge to further their economic and security interests to the detriment of Canada's. For instance, CSIS actively investigates threats of foreign interference and espionage and supports the Government of Canada's collective effort to respond, including acting to reduce the threat of specific foreign espionage activities through its lawful mandate.

In addition, foreign states, including the PRC, attempt to threaten and intimidate individuals around the world, including in Canada, through various state entities and non-state proxies. We strongly denounce this behavior wherever it may occur. We know that states may attempt to threaten and intimidate individuals in order to pursue fighting alleged corruption or to bring alleged criminals to justice. However, we are aware that these tactics can also be used as cover for silencing dissent, including on university campuses, pressuring political opponents and instilling a general fear of state power no matter where a person is located. The PRC's *Operation Fox Hunt* is one such example. The PRC uses this program as a means to identify and try to repatriate to China individuals who they allege are corrupt. The PRC has conducted this operation in Canada since 2014. I will note that as per the 2019 NSICOP report, initially the response was often to work with Chinese officials to "support their investigations of corrupt officials." However, "increasingly stringent criteria" on the People's Republic of China investigators involved in this program has been added as time passed following 2015.

When foreign states target Canadians, persons residing in Canada, or their families, they are seeking to deprive members of Canadian communities of their fundamental rights and freedoms. Such actions are unacceptable. If anyone feels intimidated or threatened it is of the utmost importance to

contact your local police, and I can assure you that your concerns will be dealt with in a serious and appropriate manner.

*Foreign interference and COVID-19*

The COVID-19 pandemic has accelerated these trends by providing foreign threat actors with unique opportunities to pursue their hostile activities. The impacts of disinformation, coercive use of trade and economic-based threats to national security, and threats to Canada's supply chain are ongoing concerns.

This past year, we have observed state-sponsored information manipulation, or disinformation by certain regimes against Canada and our allies. These campaigns aim to sow doubt about the origins of the COVID-19 virus and the means required to counter it; discredit responses to COVID-19 while casting their own as superior; and erode confidence in our shared values of democracy and human rights.

Canada's security and intelligence community, which is at the forefront of Canada's efforts to combat foreign interference, is taking coordinated and integrated action to protect the safety, security and strategic interests of Canadians. I would like to provide you with an overview of these efforts.

## CANADA'S RESPONSE TO FOREIGN INTERFERENCE

There is no more fundamental role for the Government than to keep Canadians and communities safe. The Government takes this responsibility seriously. Though I am unable to share operational information regarding ongoing counter foreign interference activities, Canadians can be confident that the Government of Canada applies a whole-of-government approach to protect Canadians from national security threats, including threats to institutions that play a key role in Canada's response to the COVID-19 pandemic.

*Investigations and monitoring*

CSIS has longstanding investigations into foreign interference threat activities that target Canada, and uses the full mandate of the *CSIS Act* to investigate, advise the government and take action to reduce the threat. CSIS works closely with other government partners, inside and outside the security and intelligence community, to address clandestine, deceptive or threatening interference activities that can pose significant harm to Canada's democratic institutions and processes.

The Royal Canadian Mounted Police (RCMP) have a broad, multi-faceted mandate that allows them to investigate, and disrupt threats from foreign actors by drawing upon various legislation, including investigations with a view to laying charges under the *Criminal Code of Canada*.

The Communications Security Establishment (CSE) provides intelligence and cyber assessments to the Government of Canada on the intentions, activities and capabilities of foreign threat actors, and can also carry out active cyber operations to degrade, disrupt, respond to or interfere with the capabilities, intentions or activities of foreign individuals, states, and organizations. CSE also provides advice, guidance, and services to help protect electronic information and information infrastructures of federal institutions and of systems of importance to the Government of Canada.

In addition, in an effort to counter foreign interference against the 2019 Federal Election, the Government created the Security and Intelligence Threats to Elections (SITE) Task Force, composed of officials from CSE, CSIS, RCMP and Global Affairs Canada (GAC). Throughout the 2019 Federal Election, the SITE Task Force raised awareness and assessed foreign interference threats, briefing members of the Government of Canada's Critical Election Incident Public Protocol on any threat activities to ensure nothing affected Canada's ability to have a free and fair election. The SITE Task Force continues to monitor and advise the Government of Canada on foreign interference-related threats to federal elections.

The Canada Border Services Agency (CBSA) works closely with its partners to ensure that individuals that pose a security threat to Canada, including those who engage in acts of espionage or acts of subversion against democratic governments, do not gain entry into Canada. Those who have previously entered and are deemed inadmissible will be removed from Canada. Through its robust Intelligence and National Security Screening programs, the CBSA aims to detect such inadmissible persons at various points in the travel continuum and advise other security and intelligence partners of possible threats.

Through investigations and monitoring, we continue to identify and shed light on the multiple ways foreign interference manifests itself in Canada, allowing us to be well-armed with the knowledge needed to deploy our tools to counter it.

*Protecting against economic-based threats to national security*

The Government has never and will never compromise Canada's national security, and will take action where necessary to protect it. As reported in the 2018-19 *Investment Canada Act* Annual Report, for the four fiscal years 2015-16 to 2018-19 the Governor in Council issued eight 25.4 final orders:

six blocking or ordering the foreign investor to divest of its investment and two imposing conditions that protect national security while allowing those investments to proceed.

To protect Canadians in this current economic environment shaped by COVID-19, the Government of Canada announced in April 2020 that it is applying increased scrutiny to all foreign direct investments, controlling or non-controlling, into Canadian businesses that are vital to public health and the security of supply of critical goods and services to Canadians or to the Government of Canada. The Government also announced that all foreign investments by state owned enterprises, or private investors assessed as being closely tied to or subject to direction from foreign governments, would be subject to enhanced scrutiny under the national security provisions of the *Investment Canada Act*. Innovation, Science and Economic Development (ISED) and Public Safety Canada work together, in conjunction with 18 other federal departments, to meet the legislative requirements of this *Act* on behalf of the Government of Canada and Canadians.

The Government of Canada purchases approximately $22B worth of goods and services each year. The potential exists for foreign threat actors to exploit procurement processes to their advantage. State-owned enterprises use their vast resources as a competitive advantage that allows them to underbid Canadian companies, and insert themselves into our infrastructure and services, and undermine our security. The Government is committed to addressing procurement-based national security threats. For example, we are working to enhance risk awareness and ensure due diligence throughout the procurement process. This has included the development of national security guidance material, which has been distributed to employees of departments and agencies with duties that include, or may be impacted by, procurement activity, as well as to Provinces and Territories, and the Canada City Alliance, which represents 12 of Canada's largest cities.

The Government is aware of the ongoing attempts by some foreign states to undermine our economy for their own benefit. Our many efforts to counter these threats help protect Canadians' prosperity and maintain Canada as an economic leader.

*Protecting our democracy*

In January 2019, the Government announced its plan to defend Canadian democracy from threats ahead of the 43rd General Election. This plan was built on four mutually supporting pillars:

1. *Enhancing Citizen Preparedness* by supporting an informed and engaged citizenry;

2. *Improving Organizational Readiness* by strengthening coordination to identify threats, emerging tactics and systems vulnerabilities;

3. *Combatting Foreign Interference* by preventing covert, clandestine or criminal activities by foreign actors aimed at interfering in our democratic processes; and

4. *Expecting Social Media Platforms to Act* by guiding social and digital platforms to ensure integrity, transparency and authenticity.

The plan was internationally recognized as illustrating Canada's leadership in countering foreign interference in democratic processes, and key components are being evaluated for on-going implementation.

In addition, the *Canada Elections* Act contains provisions that aim to protect the federal electoral process, including strong regulations related to financial and non-financial contributions to political actors, and prohibitions against bribing or intimidating electors. The *Elections Modernization* Act, which received Royal Assent in December 2018, further strengthened protections against foreign interference through amendments that:

- Prohibit third parties from using foreign funds for their partisan activities and advertising, irrespective of when it takes place;
- Prohibit foreign entities from spending any money to influence federal elections;
- Require registered third parties to have a Canadian bank account; and,
- Prohibit any organizations – online or offline – that sell advertising space from knowingly running election advertisements paid for with foreign funds.

A pre-election period was also established, extending spending limits for third parties and subjecting third parties to enhanced reporting obligations. To improve transparency, the amended law also requires online platforms such as social media sites to publish a registry of all partisan or other political advertising they have carried, including who authorized the advertisements, and to keep that information available for a minimum of two years after the advertisements are posted.

As democratic processes were being targeted in multiple countries around the world by foreign threat actors, it was clear Canada needed to take action

here at home. As a result, we took these key measures to bolster the robustness of our democratic and electoral institutions to tackle this threat head on.

*Reaching out to Canadians*

What the Government does to counter foreign interference is often done behind the scenes, given the sensitivity of the tools and techniques involved. But in light of the breadth of foreign interference and its impact on so many areas of society, our agencies have been engaging with Canadians to assist with the signs of what to look for, and who to call when they encounter it.

In this respect, CSIS provides briefings to private companies, universities and research institutions to help them better understand how to protect their work. In the context of the pandemic, Canada's security and intelligence agencies moved quickly to work with the life sciences sectors involved in Canada's response to COVID-19 to help protect them from foreign interference activities. As an example, CSIS has undertaken a national outreach campaign aimed at sensitizing these sectors from the threat they could face from foreign interference.

The RCMP also engages with the Canadian Association of Chiefs of Police to help inform local law enforcement agencies of threats from foreign interference and to establish mechanisms for reporting foreign interference incidents.

With respect to foreign interference and other cyber threats, CSE's Canadian Centre for Cyber Security (Cyber Centre) recently released the *National Cyber Threat Assessment 2020* report, which highlights cyber threats facing individuals and organizations in Canada in order to help Canadians shape and sustain our nation's cyber resilience. This includes threats from activities sponsored by countries such as the PRC, covering cyber espionage, intellectual property theft, online influence operations, and disruptive cyber incident. The Cyber Centre also provides cyber security guidance and best practices, including through CSE's Get Cyber Safe public awareness and education campaign.

The Government is committed to continued engagement with Canadians on the issue of foreign interference to build awareness and bolster resilience.

*Protecting Canadian Knowledge and Research*

The Government of Canada is committed to an open and collaborative environment for science and research, and recognizes the importance of Open Science as essential for research discoveries and innovation. At the

same time, espionage and foreign interference activities pose real threats to Canadian research integrity, intellectual property, and business interests.

Universities, government departments, the federal granting councils, and national security agencies are regularly in contact as part of ongoing engagement activities, and collaborate to understand, identify and respond to potential threats to research security. This dialogue includes a joint Government of Canada-Universities Working Group which facilitates the identification, sharing and promotion of best practices to minimize security risks, protect data and intellectual property.

As part of this work, the Government of Canada and the academic sector worked collaboratively to develop and launch an online resource portal called "Safeguarding Your Research." The portal provides information, best practices and tools to help researchers identify and mitigate potential security risks to their work. Earlier this year CSIS gave a briefing to the Canadian Chamber of Commerce which flagged China and Russia as countries actively involved in commercial espionage.

Recognizing the elevated threat of foreign actors targeting COVID-19 related research in Canada, the Government of Canada also released a policy statement on research security – signed by the Minister of Innovation, Science and Industry, the Minister of Health, and myself – in September 2020. The statement identifies the potential threats to research security and the need to take appropriate measures to safeguard research and innovation, particularly in the context of COVID-19.

Furthermore, the Government has instructed federal research funding agencies, including the Canada Foundation for Innovation, the Canadian Institutes of Health Research, the Natural Sciences and Engineering Research Council, and the Social Sciences and Humanities Research Council, to review their security policies and processes and to promote awareness of the best practices and tools available to the Canadian researchers and innovators they fund, so that Canada, rather than our adversaries, maximizes benefits from the Government's significant investments in science and research.

Additionally, direct engagement between Canadian universities, federal laboratories and security institutions on the risks posed by foreign interference has been ongoing since 2016 through the Safeguarding Science initiative led by Public Safety Canada, in partnership with 10 other federal departments.

This initiative aims to raise awareness within Canada's research communities of the risks of proliferation; dual-use technology; research security; and cybersecurity. The initiative informs participants about tools to help recognize and mitigate the risks Canadian institutions are facing, including those posed

to their research and development. Thus far, Safeguarding Science presentations have been delivered to 33 institutions and 5 federal labs across the country. Expansion efforts are also underway to deliver additional tools and guidance to the research community, along with more workshops from coast-to-coast and within the private sector and with Provincial/Territorial partners.

Public Safety Canada has also established a Federal, Provincial and Territorial Community of Practice on Economic-based National Security Threats to bring together key officials across these jurisdictions to discuss national security threats that arise through certain economic activities.

Canada's multi-disciplinary research community is world-renowned. With the right tools and awareness of the potential risks, we can ensure that Canada continues to maximize benefits from our significant investments in science and research.

I will note that just this week it was reported that CSIS has been engaging with, and briefing government partners and companies in the vaccine and other medical supply chains. I can assure you that our agencies will continue to work closely with our partners to ensure that as many businesses and orders of government have the information they need to implement pre-emptive security measures to identify and mitigate all threats.

*International collaboration*

Canada cannot tackle foreign interference alone. Our international allies and partners face similar threats. And so, by working together, we bring our collective resources to bear in countering threats from foreign actors. Canada has always stood up for a rules-based international order, one in which all countries abide by international norms. Consistent with these principles, Canada actively shares information and coordinates responses with allies through numerous multilateral bodies and relationships.

As a member of the Five Country Ministerial, I have committed to collaborating with my counterparts in the United States, the United Kingdom, Australia and New Zealand on the issue of foreign interference, to share information about our respective approaches and to coordinate responses and attribution as deemed appropriate.

Security and intelligence partners also collaborate to share information in an effort to counter foreign interference, including state-sponsored disinformation, through a number of fora. The security and intelligence community, for example, work with domestic and international partners to share information that can help detect, investigate, and prevent foreign interference in Canada.

Global Affairs Canada leads the G7 Rapid Response Mechanism. In 2018, G7 leaders committed to working together to strengthen G7 coordination to identify and respond to diverse and evolving foreign threats to G7 democracies, including through sharing information and analysis and identifying opportunities for coordinated response. The G7 RRM's focus includes, but is not limited to, threats to democratic institutions and processes; disinformation and media; and fundamental freedoms and human rights. The mechanism has since expanded to include Australia, the Netherlands and New Zealand. G7 RRM information sharing was tested and proven in the COVID-19 context. The mechanism quickly shifted its focus to the pandemic, supporting a real-time exchange of analysis of foreign threats that included industry and civil society organization partners, particularly with respect to evolving foreign state-sponsored information manipulation.

Working with our international partners, we have also taken measures to publicly attribute foreign interference activities when appropriate. For example, in December 2018, Canada again joined partners in calling out the Chinese Ministry of State Security for the compromise of Managed Service Providers (MSPs). The Cyber Center reached out to MSPs in Canada to inform them of the threat and offer assistance.

The Government of Canada is committed to working with our partners and allies to share the critical information necessary to understand and counter the full spectrum and threat of foreign interference.

*Protecting our citizens and our communities*

Canada does not tolerate harassment or intimidation of its citizens. Any allegation of harassment or intimidation is taken seriously by the Government of Canada and will be dealt with appropriately.

Any Canadian who feels threatened or intimidated by a person acting on behalf of a foreign country is encouraged to contact their local police at the earliest possible opportunity. In instances where this threat rises to a level where individuals are concerned for their personal safety and security, it is essential that they report this information to local law enforcement agencies for their immediate action.

Through Integrated National Security Enforcement Teams our national security agencies investigate national security matters domestically and internationally. CSIS collects evidence and provides intelligence advice. The Police of Jurisdiction, including the RCMP, has the authority and expertise to investigate cases whereby the evidence supports it. Canadians who are concerned that they are being targeted by state and non-state actors for the purposes of foreign interference should contact the RCMP's National Security

Information Network at 1-800-420-5805, or by email at RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca.

Canadians may also report information related to foreign interference to CSIS by contacting 613-993-9620, or by completing the web form at: www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html.

Our law enforcement and security agencies are actively engaged in protecting Canadians from these threats. Canadians should feel confident that they have the skills, resources and capabilities to do what it takes to keep them safe.

*Moving Forward*

Colleagues, I welcome the interest you and other members of the House of Commons have shown in how the Government of Canada addresses foreign interference. Bringing these issues to the attention of Canadians and raising awareness amongst stakeholders is key to countering this threat.

It is only through raising awareness, building resilience, forging partnerships with key stakeholders and seeking innovative ways of responding to threats that we will be successful in countering the evolving and complex nature of foreign interference. We are therefore always looking for new ways of doing things, and meeting this challenge head on.

This Government values above all the wellbeing and safety of Canadians. Whenever malign foreign states seek to harm our communities, undermine our values or jeopardize the very institutions on which our country is built, we will take action. We cannot always make Government actions public in this sphere, but our sustained efforts make a difference in the lives of Canadians.

Sincerely,

The Honourable Bill Blair, P.C., C.O.M., M.P.