Minister of Public Safety Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

Colleagues,

As you know, foreign interference is a threat to Canada and Canadians, which is why it should be an area of significant focus for members of this Parliament.

Foreign interference affects officials and staff at all levels of government (federal, provincial/territorial, and municipal), and targets all facets of Canadian society, including civil society, Canadian communities, the private sector, academia, media, and our democratic institutions, including elections. It is our collective responsibility to ensure that Canada and Canadians are resilient and are equipped to protect themselves against foreign interference.

Several factors make Canada an attractive target of foreign interference: our promotion of democracy and human rights, our advanced economy and intellectual property, our membership in a number of international fora, and being a home to diverse and multicultural communities. We bear witness to foreign state actors leveraging all elements of their state power to advance their political, economic and military objectives, posing direct threats to our national security and sovereignty. This threat activity is being observed at levels not seen since the Cold War.

Canada's democratic institutions and processes are strong and the Government of Canada actively works to ensure their continued protection. Above all else, respect for the rule of law, the promotion of Canadian values and principles, and the protection of Charter rights and freedoms is at the heart of our approach in countering foreign interference. Accountability and transparency is of paramount importance to ensure that Canadians trust in their elected officials and democratic system of government.

An important step we must take collectively is to be aware that Parliamentarians and our staff are of immediate and heightened interest to certain foreign state actors seeking to interfere in Canada's democratic institutions and processes. Foreign state actors know that Parliamentarians in Canada yield influence, and have access to decision-makers as well as privileged and sensitive information. We must remain aware of the tradecraft used to target not only officials but also the Canadian public, media, voters, political parties, and candidates and staff, both outside of and during an election.

The nature of foreign interference threats means that all Canadians have a role to play in protecting Canada's democracy and national security. Simply put, an informed and engaged society bolsters our defences against foreign interference.

[APG]

In July 2021, the Canadian Security Intelligence Service (CSIS) released a public report on Foreign Interference Threats to Canada's Democratic Process to raise awareness and build resilience against foreign interference amongst all Canadians. If you have not already done so, I invite you and your staff to review this material. A section of this report serves to describe the techniques foreign states use to conduct foreign interference. I have outlined these in brief below:

- Elicitation results when a targeted person is manipulated into sharing valuable information through a casual conversation. For example, a threat actor could knowingly seek to provide someone with incorrect information, in the hope that the person will correct them, thereby providing the information the threat actor was actually looking for. A threat actor may also share some form of sensitive information with the individual in the hopes that the individual will do the same. You can help avoid it by being discreet, by not "over-sharing", and by assuming public conversations are monitored.

- Cultivation is when threat actors seek to build long-lasting, deep, and sometimes even romantic relationships with targeted persons. These relationships enable the manipulation of targets when required, for example, through requests for inappropriate and special "favours". To establish a relationship, the threat actor must first cultivate a target. Cultivation begins with a simple introduction with the end goal of recruitment over time. Shared interests and innocuous social gatherings are often leveraged. You can help avoid it by being aware and keeping track of unnatural social interactions, frequent requests to meet privately, out-of-place introductions or engagements, gifts and offers of all expenses paid travel.

- Coercion, including blackmail and threats are among the most aggressive types of recruitment. If a threat actor acquires compromising or otherwise embarrassing details about a target's life, they can seek to blackmail the person. Sometimes, blackmail or threats may occur after a long period of cultivation and relationship-building. A threat actor may also attempt to put someone in a compromising situation, just to blackmail the person later. Threat actors may also use covert operations, such as intrusions, to steal or copy sensitive information and later use that information to blackmail or threaten the individual. You can help avoid it by not sharing compromising details or personal information with untrusted individuals, both in-person and online.

- Illicit and Corrupt Financing happens when threat actors use someone as a proxy to conduct illicit financing activities on their behalf. Inducements may occur innocuously via a simple request for a favour. For example, a threat actor may ask a target to "pay someone back" or relay money to a third party on their behalf. Political parties and candidates may also receive funds (e.g., donations) seemingly from a Canadian citizen or permanent resident,

[APG]

that may have originated from a foreign threat actor. You can help avoid it by being aware of inappropriate requests which involve money, and questioning the source of suspicious donations or "gifts".

- Cyber attacks can compromise electronic devices through a range of means. Socially-engineered emails (i.e., spear-phishing emails) can trick the recipient into clicking a specific link thereby sharing details about their devices, or can potentially introduce harmful malware into their systems. These cyber attacks enable threat actors to collect potentially useful information (e.g., voter data, compromising information about a candidate) that can be used in a foreign influenced operation. You can help avoid it by using strong passwords, enabling two-factor authentication, and not clicking on links or opening attachments unless you are certain of who sent them and why.

- Disinformation occurs when threat actors manipulate social media to spread disinformation, amplify a particular message, or provoke users (i.e., "troll" users) when appropriate to serve their interests. A growing number of foreign states have built and deployed programs dedicated to undertaking online influence as part of their daily business. These campaigns attempt to influence public opinion, civil discourse, policymakers' choices, government relationships, the reputation of politicians and countries, and sow confusion and distrust in Canadian democratic processes and institutions. You can help avoid it by being critical of what you are consuming online, careful what you share (or repost from others), and taking note of unexpected online interactions.

- Espionage, while distinct, is often used together with foreign interference to further threat actors' goals. For instance, information collected or stolen through espionage can be very useful in planning and carrying out a foreign influence or public disinformation campaign. You can help avoid it by following security of information protocols, not disclosing information to individuals who don't have a reason to access it, and being discreet about how you handle sensitive information.

With respect to foreign interference related cyber threats, the Canadian Centre for Cyber Security (Cyber Centre) released the *National Cyber Threat Assessment* 2023-2024. You may also wish to familiarize yourself with this 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 such as cyber espionage, intellectual property theft, online influence operations, and disruptive cyber incidents.

In addition, CSIS, the Communications Security Establishment (CSE), the Royal Canadian Mounted Police (RCMP), Global Affairs Canada (GAC), have provided, and

will continue to provide, classified threat briefings to political party leadership during electoral periods when required and as needed. These briefings are intended to contribute to the strengthening of our internal security practices, and to build awareness of foreign-influenced activities in Canada. The frequency of these briefings will continue to be balanced with the operational responsibilities of these departments and agencies.

As you can see, the threat environment is complex and diverse. The Government of Canada leverages many tools and actively takes measures to investigate, counter and prevent foreign interference threats. And, importantly, there are mechanisms in place to report foreign interference. If you are concerned that you, members of your staff, or members of your constituency, are being targeted by a foreign state or state-linked actor, report it. You can contact CSIS at 613-993-9620 or 1-800-267-7685, or by completing the web form at www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html.

In addition to contacting their local police, any individual in Canada who is concerned that they are being targeted by state or non-state actors for the purposes of foreign interference may 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.

And, as always, to report a threat or immediate danger, call 9-1-1 or contact local police.

I want to conclude this letter by stating, clearly and unequivocally, that for the sake of our national security and sovereignty, and indeed, ensuring that Canadians trust our electoral processes, foreign interference, including acts targeting our democratic institutions and electoral processes, is not a partisan issue. Foreign interference is an increasingly sophisticated global issue and in Canada, elected officials across all levels of government, representing all political parties, are potential targets of foreign interference. I am here to hear your concerns, and I will make myself available to do so.

As Parliamentarians and leaders, it is our responsibility to protect Canada and Canadians from the threat of foreign interference. Together, we can protect Canadian values, rights and freedoms and ensure the integrity of our democratic institutions, and civil and political system from those who seek to harm our way of life.

Yours sincerely,

[APG]

The Honourable Marco E. L. Mendicino, P.C., M.P.