PROTECTED B
FOR OFFICIAL USE ONLY

Foreword

As the Minister of Public Safety, and on behalf of all federal partners, I am pleased to present Canada's first *Counter-Foreign Interference Strategy*. The *Strategy* will strengthen Canada's defences against foreign interference and enhance the Government's ability to respond in a decisive and firm manner.

Foreign interference is a serious threat. Foreign states, or entities operating on their behalf, have made efforts to influence Canadian elections and subvert both elected and unelected officials. Threat actors have weaponized social media networks to spread false information harmful to Canadian interests and they have used espionage and sabotage to gain unfair advantages over Canada's business, industry, and research sectors. Members of Canada's diverse cultural communities have reported disturbing cases of intimidation and harassment. None of this is acceptable.

The Government of Canada is committed to using every available resource to neutralize this threat and hold its perpetrators to account. The *Strategy* builds upon existing federal efforts by aligning them with the principles of deterrence, strength, and action.

Because combatting foreign interference demands a whole-of-society approach, Public Safety will partner with other government departments, including at other levels of government, our international allies, and with civil society and the private sector. We commit to ensuring that the Canadian public is well-informed and able to access the tools available to them through this and other government resources. Transparency is at the heart of our approach. We seek to shine a light on foreign interference in Canada and to share what the government is doing in response.

The *Strategy*'s core goals are reflected in the substantial investments made in Budget 2023 to counter foreign-interference. These include new investments in the Royal Canadian Mounted Police and $13.5 million over the next five years plus $3.1 million ongoing to establish a National Counter-Foreign Interference Office, housed at Public Safety.

The Government of Canada is committed to protecting the safety and security of its citizens against this evolving threat. The *Counter-Foreign Interference Strategy* is the roadmap for Canada's path forward. We are proud to be leading the way.

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

[APG]

PROTECTED B
FOR OFFICIAL USE ONLY

Canada's Counter-Foreign Interference Strategy

A Strategy to Protect Canadians and Canadian Values

Foreign interference is one of the foremost strategic threats to Canada's national interest and security. It poses a direct threat to our sovereignty, democratic institutions, fundamental rights and freedoms, prosperity, and security. Threat activities observed target all levels of government, the private sector, academia, communities and the public.

The goal of Canada's *Counter-Foreign Interference Strategy* is to defend Canadian sovereignty, values and interests from foreign interference, and make Canada more resilient to this threat. To achieve this goal, the Government of Canada will pursue three lines of effort — *Detect, Strengthen, and Act* — with a focus on five priority sectors to:

- ensure our democracy remains strong and secure;
- protect Canadians and our communities;
- safeguard our prosperous economy and scientific excellence;
- uphold fundamental Canadian values both at home and abroad; and
- defend the integrity of our supply chains and critical infrastructure.

Canada's National Counter-Foreign Interference Coordinator, housed at Public Safety Canada, will coordinate the implementation of the *Counter-Foreign Interference Strategy*, to give Canada's existing and future collective efforts greater focus, coherence and effect.

A More Sophisticated, Persistent and Pervasive Threat

Foreign interference includes activities undertaken by foreign states, or entities acting on their behalf, to advance their own strategic objectives to the detriment of Canada's national interests. It includes activities that fall below the threshold of armed conflict, yet are clandestine, deceptive, threatening and/or illegal. Foreign interference is distinct from normal state activities to exert influence, which are legitimate, legal and an integral part of conventional and rules-based international relations.

Normal activities to exert influence: Representatives from Country A openly and transparently engage with Country B to promote issues of importance to Country A, for example the respect and promotion of human rights in Country B.

Foreign interference: Country A directs an influential public figure or group to publicly promote Country A's position on a certain contentious international issue to influence Country B, without disclosing their ties to Country A. This is the threshold that constitutes foreign interference.

Foreign interference is increasingly sophisticated, persistent and pervasive. In a context of growing global competition, some foreign states are leveraging all tools at their disposal - from social media to intelligence agents - to advance their political, economic,

[APG]

technological, and military interests. This includes the use of proxies or non-state actors to allow for plausible deniability and to avoid being held to account.

Detect, Strengthen and Act

The Government of Canada has a fundamental responsibility to protect Canada's national security, the security of the Canadian public and the integrity of public institutions. Canada's security and intelligence community to counter foreign interference has been working diligently for decades, often outside of the public eye, to protect our country. To learn more about what the Government of Canada is doing to counter foreign interference, and the mandates that guide them, please see Foreign Interference (publicsafety.gc.ca).

Canada's *Counter-Foreign Interference Strategy* adopts a whole-of-society approach to increase Canada's resilience and ability to counter the threat of foreign interference in a way that upholds Canadian law, values, and fundamental rights and freedoms. The Government of Canada has a number of robust, and longstanding efforts that contribute to each of these pillars, some of which are outlined below.

1. **DETECT**: The Government of Canada collects and analyzes information on foreign interference and those who perpetrate it. This can also include important information provided by public reporting on foreign interference. The **DETECT** pillar supports the Government of Canada's response by providing our security and intelligence agencies with the information they need to pursue leads and investigations.

To **DETECT** foreign interference, the Government of Canada:

- Leverages covert and open source intelligence capabilities to collect, analyze and provide advice across the Government of Canada on threat activities;
- Investigates foreign interference activities in accordance with applicable laws while respecting rights protected under the *Charter of Rights and Freedoms*;
- Conducts national security reviews of foreign investments that may threaten Canada's national security under the *Investment Canada Act*;
- Reviews research grant applications to protect Canadian research and intellectual property from unwanted transfer;
- Provides foreign signals intelligence and assessment on the intentions, activities, and capabilities of foreign threat actors under the *Communications Security Establishment (CSE) Act*;
- Strengthens collaboration with all levels of government (Indigenous, provincial, territorial, and municipal) to promote a collective awareness of FI threats and enable threat reporting and identification;
- Enhances the public's ability to be aware of and expose foreign interference through reporting mechanisms and information products; and
- Collaborates with allies and like-minded states to exchange threat information.

[APG]

Every individual in Canada should feel free to express their political views and religious beliefs without fearing for their safety, including foreign state-backed repression. It's important for those who may be targeted by foreign states to know that they are not alone. The Government of Canada has various reporting mechanisms that are confidential, safe and anonymous for anyone who would like to report a suspected threat. To learn more, please refer to the *Preventing, Recognizing And Exposing FI* annex.

2. **STRENGTHEN:** The Government of Canada works to bolster our defences and societal resilience by increasing awareness of the threat, and reducing vulnerabilities and the perception of a permissive environment. The **STRENGTHEN** pillar supports the Government of Canada's response by making it more difficult for threat actors to target Canada in the first place, and makes Canadian society and institutions more resilient to incidents of foreign interference when they do occur.

To **STRENGTHEN** Canadian society against the threat of foreign interference, the Government of Canada:

- Provides information and guidance to the Canadian public, including vulnerable communities, to build whole-of-society resilience through transparency and awareness;
- Engages with the private sector, which owns and operates the majority of Canada's critical infrastructure, and all levels of government (provincial, territorial, municipal and Indigenous) to provide security assessments and further secure critical supply chains;
- Protects government systems and other cyber networks designated as important to the Government of Canada;
- Promotes public resilience and media literacy to equip the Canadian public with the knowledge and tools required to critically assess information and to improve their ability to spot manipulative content;
- Engages with a variety of stakeholders, including research institutions, academia and the private sector, to promote awareness of the tools at their disposal to safeguard their work and proprietary information;
- Works with like-minded states and allies to share lessons learned and best practices on counter-FI measures to adapt to evolving threats; and
- Continues to assess current measures, including legislation, to ensure our security and intelligence community is well-placed to address evolving threats.

[APG]

In anticipation of the 2019 election, the Government announced the Plan to Protect Canada's Democracy, comprised of four pillars: 1) Enhancing citizen preparedness; 2) Improving organizational readiness; 3) Combatting foreign interference; and 4) Building a healthy information ecosystem. Building on the success of these initiatives in 2019, key measures were improved and renewed for 2021 and beyond.

3. **ACT:** The Government of Canada uses all appropriate tools to respond to foreign interference, based on intelligence and information, in accordance with the law. The **ACT** pillar supports the Government of Canada's response by taking concrete and tangible actions against foreign interference.

To **ACT** in order to prevent and disrupt foreign interference, the Government of Canada:

- Investigates suspected illegal activities related to foreign interference and seeks to address them through criminal or other charges in accordance with Canadian laws (e.g., *Criminal Code, Security of Information Act, Canada Elections Act*);
- Conducts threat reduction measures under the *Canadian Security Intelligence Service Act,* both in Canada and abroad, to reduce and mitigate threats to Canada's national security;
- Takes action where necessary under various legislation (e.g., *Investment Canada Act*) to ensure the integrity of investments into and exports from Canada;
- Denies entry or status to individuals deemed inadmissible on national security grounds (e.g., persons engaging in espionage) under the *Immigration and Refugee Protection Act* and *Citizenship Act* – or removes individuals subsequently deemed inadmissible due to these threats;
- Conducts defensive cyber and active cyber operations (authorized under the *CSE Act*) to protect federal or other cyber networks designated as important to the Government of Canada, and to disrupt and interfere with the activities of foreign threat actors;
- Shares cyber threat information and mitigation advice with the operators of critical networks and deploys, upon request, cybersecurity tools to help defend networks;
- Publicly denounces and attributes foreign interference to specific states, where and when appropriate;
- Uses a number of calibrated diplomatic options ranging from formal messaging to the reduction or suspension of engagement with states that engage in foreign interference;
- Imposes sanctions under the *Special Economic Measures Act* and the *Justice for Victims of Corrupt Foreign Officials Act* (Sergei Magnitsky Law); and
- Coordinates diplomatic and operational responses with like-minded states and allies where appropriate to develop and expand collective responses to foreign interference.

[APG]

PROTECTED B
FOR OFFICIAL USE ONLY

Following a British investigation which revealed that Russian intelligence services used a nerve agent to poison a former Russian spy and his daughter in 2018, the Government of Canada announced the expulsion of four Russian diplomats who used their diplomatic status to undermine Canada's security or interfere in our democracy. Canada further denied Russia three applications for additional staff for similar reasons. Ultimately, 29 countries expelled a total of 145 Russian officials. Canada also released a joint statement alongside France, Germany, the United States, and the United Kingdom publicly attributing this event to the Russian military intelligence service.

[APG]

PROTECTED B
FOR OFFICIAL USE ONLY

Priority Sectors that Require Enhanced Protection

The *Strategy* identifies five priority sectors requiring enhanced protection owing to their importance to Canada's national interest.

Democratic Processes and Government Institutions: Threat actors attempt to undermine our democratic values, processes and institutions to promote their interests. Foreign interference can mean targeting politicians and public servants, as well as their families and those close to them, at all levels of government including Indigenous, federal, provincial, territorial and municipal levels; conducting malicious cyber operations against government networks; or spreading disinformation aimed at influencing voter opinions, public discourse, and policymaking. These activities erode public confidence in Canada's electoral processes and public institutions, and undermine the public's ability to make free and informed decisions.

Country A offers to provide support to a candidate or political party during an election that it perceives as more aligned with Country A's interests, despite such support potentially violating election law. This can include funding to hire campaign staff, engage in political organizing, and buy advertisement time. Concurrently, Country A spreads false or misleading information about a candidate or political party it perceives as more adversarial.

Communities: Canada's free, open, multicultural and inclusive society makes it a target of foreign interference. Communities in Canada are targeted by threat actors who threaten or use coercive measures to undermine free speech in the media and academic institutions. They seek to silence dissent, manipulate the narrative on certain divisive issues, pressure political opponents and instill fear among Canada's diverse communities. These activities subvert the security, human rights and fundamental freedoms of persons in Canada, including those who have come to Canada seeking the guarantee of these rights.

Country B has established offices in Canada under the guise of providing services ~~to members of its diaspora communities~~to persons in Canada with whom it shares an ethnic or national connection, without declaring this to the Government of Canada. Country B may leverage these offices to monitor and intimidate individuals who engage in activities that Country B views as contrary to its interest.

Economic Prosperity and Research Security: Canada's strong economy and world-class research community allow businesses to innovate, succeed and prosper, delivering strong economic growth that benefits all. Threat actors use both licit and illicit means to obtain high-value goods, research, sensitive information,

[APG]

data and technology. Canadian companies in almost all sectors of our economy have been targeted. Research that provides military, security, intelligence capabilities or other strategic advantages are of particular interest to threat actors. These activities jeopardize Canada's national security and defence, and its ability to innovate and compete, resulting in lost jobs and diminished economic growth.

Country C uses various means, including social media, to recruit Canadian academics and experts in science, technology, engineering and mathematics (STEM) fields and rewards them for transferring proprietary information to Country C. This can include findings from publicly funded research.

International Affairs and Defence: Canada is an active promoter of democracy, the rule of law, inclusivity, and human rights around the globe, and a protector of the international rules-based system. Canada's diplomatic corps and the Canadian Armed Forces are frequently on the front lines of these efforts. Threat actors may target Canadian foreign policy interests abroad, including diplomatic and military assets and personnel abroad. These hostile activities aim to undermine Canada's ability to promote its interests and values on the international stage. Some foreign states also seek to leverage international bodies and authorities to shape norms, laws, and standards in their favour to the detriment of Canada and others.

Country D creates fake social media accounts impersonating Canadians to covertly push its narrative in Canada and amplify content shared by Country E's officials. These accounts may also be used to promote content from conspiracy publications and inauthentic news sites aimed at discrediting Canada's international policies or Canadian personnel posted abroad.

Country E has been increasing its presence in the Arctic region through the deployment of research vessels that it claims are used to conduct research on climate change. However, these vessels may be using scientific research as a cover to conduct surveillance operations in Canadian waters.

Critical Infrastructure: Critical infrastructure (CI), such as energy, transportation and telecommunications, enables Canadians to go about their everyday lives. Threat actors may target our CI systems to undermine confidence of Canadians in their government, and/or to damage our economy. Many of Canada's CI systems are interconnected with one another, across provinces, territories, and with other countries. An exploitation of a vulnerability in Canada's CI could also have cascading effects. These activities disrupt the supply of critical goods and essential services necessary to the well-being and security of persons in Canada, and weaken the public's confidence in Canada's CI.

[APG]

Country F employs hackers to deploy cyber operations against a Canadian gas distribution operator to collect sensitive information and gain access to its system to disrupt services or cause physical damages.

An Ongoing Commitment

As the Government of Canada implements this *Counter-Foreign Interference Strategy*, it will continue to assess our national approach to ensure it adapts to evolving threats. This includes the continuous evaluation of the tools and measures at the Government of Canada's disposal, including the advice provided by national security review bodies.

The Government of Canada's *Counter-Foreign Interference Strategy* is anchored in a whole-of-society approach, which will leverage Canada's strong institutions, diverse society, and robust partnerships with all levels of government and partners around the world.

Canada's unyielding commitment to the rule of law, democracy, and the respect for rights and freedoms enshrined in the *Canadian Charter of Rights and Freedoms* are core strengths and values underpinning Canadian society, and their preservation will be the ultimate measure of success for the *Counter-Foreign Interference Strategy*. Actions taken by Government of Canada to counter foreign interference may not always be visible, but the Government is committed to operating with as much transparency as possible and uphold the very laws and values that threat actors seek to undermine.

[APG]

PREVENTING, RECOGNIZING AND EXPOSING FOREIGN INTERFERENCE

As an advanced economy and an open and free democracy, Canada has long been the target of foreign interference (FI). The Government of Canada does not tolerate these harmful activities and pursues a whole-of-society approach to safeguarding our communities, democratic institutions, and economic prosperity. This includes enhancing citizen preparedness by ensuring Canadians have the knowledge and tools to be able to recognize and to report FI when

PROTECTING YOURSELF

Threat actors use a variety of techniques to target all aspects of civil society, including :

- Diverse communities;
- Electoral processes;
- Post-secondary campuses;
- Cutting edge research and development;
- Private companies; and,
- Traditional and social media.

Common techniques or activities used by threat actors can include: elicitation, cultivation, coercion, illicit financing, cyber-incidents, intimidation and disinformation. Learn how to recognize these common techniques and protect yourself by referring to the Canadian Security Intelligence Service's (CSIS) Foreign Interference and You publication. Also, see Get Cyber Safe.

Threat actors also target Canada's democratic process, both outside of, and during an election. To learn more about what you can do to help safeguard the integrity of Canada's democratic process, visit the Fact Sheet for Canadian Voters: Online Influence Activities, and CSIS' report on Foreign Interference Threats to Canada's Democratic Process.

HAVE A CONCERN? REPORT IT.

PROTECTING YOUR RESEARCH AND INTELLECTUAL PROPERTY

Foreign interference can include activities aimed at obtaining innovative Canadian research and development and intellectual property, including in the following fields:

- Sensitive and dual-use technologies;
- Early stage science, technology, engineering and mathematics (STEM) field research or commercial environments (e.g., start-ups);
- Big data and personal information analytics; and,
- Critical infrastructure.

It is important to remember that:

- Knowing who is in control and who will benefit from partnerships and investments is critical.
- Businesses and research institutions of all sizes are targeted – even if you are small, your work can be of value.
- Espionage and the misappropriation of research not only threaten the livelihood of Canadian businesses and institutions but pose significant long-term threats to Canada's prosperity.

Learn more about protecting your knowledge and innovations:

- Safeguarding Your Research online portal;
- National Security Guidelines for Research Partnerships;
- Mitigating economic and/or geopolitical risks in sensitive research projects guidance document.

HAVE A CONCERN? REPORT IT.

HOW TO REI INTERI

The Royal Canadian M Communications Secur Canada Border Service and online reporting me for anyone who would l national security, includ

To report suspicious inc concern to national sec National Security Inforn 5805, or by email at RC RISN.GRC@rcmp-grc.

To report non-urgent pc threats or suspicious ac 993-9620, or 1-800-267 web form.

To report non-urgent pc or incidents, contact the Security at 1-833-CYBE complete a form throug

To report non-urgent su activities, contact CBSA 888-502-9060.

To report a threat or im contact local police.

[APG]

HAVE A CON