Key Points for SITE Briefing to Political Parties

Slide 1 – Title

Slide 2 – Purpose and Objectives of this Briefing

- The purpose of the presentation today is to provide you with a comprehensive and up-to-date briefing on foreign interference.
- In the following presentation we will:
  - provide a quick refresher of SITE;
  - define the threat of foreign interference;
  - define the roles and responsibilities in countering foreign interference;
  - provide concrete examples of such interference; and
  - provide tools and resources to help you to protect yourself.

Slide 3 – SITE Construct

- The Security and Intelligence Threats to Elections (SITE) Task Force was established with a mandate to focus on examining FI in elections. **The task force works to ensure coordinated information sharing, alignment and awareness on matters related to foreign interference and elections**. SITE was active in both 2019 and 2021.
- The task force is comprised of members from the Communications Security Establishment (CSE), Canadian Security Intelligence Service (CSIS), Global Affairs Canada (GAC) and Royal Canadian Mounted Police (RCMP), with the Privy Council Office DI and S&I participating as observers.
- In parallel with FI, the SITE TF also monitor domestic terrorism threats in the context of its possible impact on election security.
- More recently, PM's direction, SITE has also been mandated to be active during federal by-elections.
- CSIS is currently the Chair of the Security and Intelligence Threats to Elections Task Force (SITE TF).

Slide 4 – Durham By-Election: Current posture

- Although SITE has previously only been stood up for the federal elections, more recently, we have been stood up for by-elections, this time included.
- SITE TF ongoing monitoring, weekly meetings
- Reporting and briefing mechanisms at classified levels

Slide 5 – What is foreign interference?

- The Government of Canada defines **foreign interference** as malign activities undertaken by states, or their proxies, to advance their own strategic objectives to the detriment of Canada's national interests.
- Examples of FI includes attempts to covertly influence, intimidate, manipulate, interfere, corrupt or discredit individuals, organizations and governments to further the interests of a foreign country. These activities, carried out by both state and non-state actors, are directed at Canadian entities both inside and outside of Canada, and directly threaten our national security.

Slide 6 – Foreign Influence versus interference?

- FINF = normal diplomatic conduct or acceptable foreign-state actor lobbying. Healthy part of diplomatic relations.
- **FINT = when foreign states conduct activities that attempt to clandestinely or deceptively manipulate Canada's open democracy and society**. Well cover later FI tactics and techniques

Slide 7 – Why Canada?

- Many characteristics make Canada an attractive target: the abundance of natural resources, advanced technology, human talent, and expertise.
- Our close relationship with the United States, our status as a founding member of the NATO and our participation in a number of defence and trade agreements, including the Fives Eyes community, has also made it an attractive target for FI.

- In addition, certain foreign powers are known to leverage Canada's multiculturalism for their own benefit in clandestinely manipulating Canadian communities.
- Canada is, most importantly, an open society. **Being an open society does carry increased risk for infiltration by foreign threat actors who could take advantage of the open nature of Canadian politics** and exploit administrative gaps associated with core Canadian freedoms.

Slide 8 – What is the GoC doing to protect against FI? (CSIS, CSE, RCMP, GAC)

- The Government of Canada takes a whole-of government approach to countering foreign interference.
- Rooted in international best practices, the Government of Canada created last year the National Counter-Foreign Interference Coordinator at Public Safety Canada to ensure coordination across the Government on matters related to foreign interference.
- *Canadian Security Intelligence Service (CSIS):* collected intelligence on FI threats (amongst others) all year long, assess them, advises the Government of Canada on those and undertakes measures to disrupt and reduce such threats.
- *Communications Security Establishment (CSE) and the Canadian Centre for Cyber Security (CCCS):*
- *Royal Canadian Mounted Police (RCMP):* GREG.
- *Global Affairs Canada (GAC):* ROBIN.

Slide 9 – Who are the targets?

- FI activities are persistent, multi-faceted, and target all areas of Canadian society.
- Canada's fundamental institutions (e.g. academia, free press, democratic institutions), governance processes, and diverse Canadian communities.
- On university campuses, states may seek to exert undue influence, covertly and through proxies, by harassing dissidents and suppressing

academic freedoms and free speech that are not aligned with their political interests.

- Similarly, states may attempt to influence public opinion and debate in Canada through interference in our press or online media.
- One of the key sectors targeted by FI activities is **Canada's democratic institutions and processes**. For instance, certain foreign states and their proxies may use foreign interference to undermine Canada's electoral process, both outside of, and during an election. Such activities may target the Canadian public, media, voters, political parties, candidates, elected officials and their staff, and elections themselves.

Slide 10 – Targets of FI: Elected and Public Officials

- Elected officials include:
  - members of Parliament;
  - members of provincial legislatures;
  - municipal officials; and
  - representatives of Indigenous governments.
- Public servants, ministerial and political staff, and others with input into, or influence over, the public policy decision-making process
- Electoral candidates and their staff

Slide 11 – What threat actors want from you?

- FI activities seek to sow discord, disrupt our economy, bias policy development and decision-making, and to influence public opinion.
- In many cases, clandestine influence operations are meant to support foreign political agendas or to deceptively influence the targeted country's policies, official, research institutions or democratic processes.
- The FI activities intend to have **you** to support or suppress specific policy positions, use you to obtain access to policy makers and other high-value targets, and attempt to obtain privileged information from you that would help them achieve their goals:

- Information about government policies and plans.
- Information about people in power positions.
- Information about security protocols.

Slide 12 – Who are the prominent threat actors?

- **China,** using a combination of overt and clandestine means and seeks to exert influence internationally.
- To do so, the PRC can use proxies to reach out to policymakers, purchase businesses in key sectors to secure its long term access to resources and technology, and meet with universities to discuss mutually beneficial exchange programs.
- In 2017, the National Intelligence Law was passed in China. This law obligates individuals, organizations, and institutions to assist the PRC security and intelligence services in carrying out a wide variety of intelligence work (compels Chinese businesses operating overseas, specifically technology companies, to hand over to intelligence agencies user data even when operating in foreign jurisdictions – as Canada).
- Community groups can also be used to exert influence on behalf of the Chinese government; these groups can be directed by officials to lobby on their behalf and support certain stances held by the Chinese government. Further, they can be used to identify those individuals who are not supportive of the Chinese government or who are not willing to act on its behalf, leading to potential consequences.
- The Chinese government seeks to monitor dissident groups (the 5 Poisons - support to Uyghur, Tibet independence, Falun Gong, Taiwan movement and Chinese democracy movement). Community groups are

asked to marginalize members of those groups amongst others in the community, or participate in activities to counter them. Such FI activities can take place on university campuses.

- One of the objectives of PRC FI is to ensure elected officials at all levels of gov't do not associate with Five Poisons. This deprives Canadians of a voice and political access and representation.

- **Russia:** As part of its FI operations, Russia carries out disinformation and propaganda efforts in the West to advance its strategic objectives.
- For instance, the Russian intelligence services (RIS) and other state-linked actors conduct disinformation campaigns to:
    - Undermine public faith in Western democratic institutions
    - Sow discord, stoke fear and anxiety, and weaken cohesion in Western democracies. (France very recently uncovers a vast Russian disinformation campaign in Europe designed to spread "deceptive or false" content about the war in Ukraine)
- Further, individual contributors act as witting and unwitting proxies and amplifiers promoting Kremlin narratives on topics that include:
    - the role of NATO in international affairs;
    - the war in Ukraine;
    - divisions and weaknesses of Western societies;
    - migration;
    - elections in Western democracies

- **Iranian FI** efforts are guided by the central goal of regime preservation.

- Iran does not tolerate any domestic dissent or criticism or advocacy against the regime that calls into question the basic tenets of Iran's political system. The Iranian regime regards Canada-based criticism, lawful advocacy and dissidents as threats and has sought to neutralize this perceived threat.
- The monitoring and intimidation of the Iranian community is a key component of Iranian FI against Canada as it is home to a relatively large and growing Iranian Canadian community.

- **India FI** is not dissimilar to approaches taken by China in terms of creating a single narrative or consistent message that helps to ensure the survival and prosperity of the foreign state. It is geared toward protecting and promoting pro – India narratives and objectives and countering activities by the diaspora communities that are viewed as counter to their national interests, such as agricultural reforms in India in late 2021 and lawful advocacy for issues such as an independent Khalistan.

Slide 13: Common FI tactics and techniques

- **Elicitation** is when a targeted individual is manipulated into sharing valuable information through a casual conversation. A threat actor could knowingly share with this individual incorrect information, in the hope that the person will correct them, or may also share some form of sensitive information in the hopes that the individual will do the same.

- **Cultivation:** threat actors seek to build long-lasting, deep, and even romantic relationships with targets, while often concealing their affiliation to a foreign state. These relationships enable the manipulation of targets when required, for example, through requests for inappropriate and special "favours".

    - For example, threat actors, including the PRC and India, seek to develop relationships with MPs, provincial legislators, and municipal officials in order to influence them to adopt certain positions or vote in a certain way.

- **Blackmail & threats** are an aggressive and common activity impacting Canada's diverse communities.

    - For example, through operations such as FoxHunt and SkyNet, alleged dissidents or economic fugitives in Canada and elsewhere are coerced in returning to the PRC via threats to their family members or associates in that country. This type of **transnational repression** is meant to intimidate and instill fear.

- **Illicit and corrupt financing.** This may occur via a simple request for a favour. A threat actor may ask a target to "pay someone back" or relay money to a third party on their behalf. Such financing can include a chain of intermediaries and proxies, some of whom may be unwitting.
    - For example, we have seen political parties and candidates receive donations, seemingly from a Canadian, though actually originating from a foreign threat actor like the PRC.

- **Cyber attacks:** Threat actors can compromise electronic devices through a range of means, such as socially-engineered emails and other malware. These cyber attacks enable threat actors to collect potentially useful information. **CSE will speak in larger details on this.**

- **Social Media Manipulation / Disinformation:** Threat actors can manipulate social media to spread disinformation, amplify a particular message, or provoke users (i.e., "troll" users) when appropriate to serve their interests. Unwitting third parties often unintentionally advance these campaigns by sharing disinformation. **GAC will present examples.**

Slide 14: Cultivation and Financing: Christine Lee and UK MP

- Christine Lee has been the subject of a 2022 MI5 Security Alert.
- Lee is prominent example of a Chinese influence agent who infiltrated the UK political landscape. UK MP Barry Gardiner had befriended Lee, a UK based lawyer, who was an alleged Chinese agent aspiring to interfere in UK politics. She had donated about half a million

pounds to support his work. Lee's friendship with MP Gardiner gave her access across the highest levels of political spectrum. Lee facilitated financial donations to political parties, Parliamentarians, aspiring Parliamentarians, including facilitating donations to a political entities on behalf of foreign nationals.

- Her activities had been undertaken in covert coordination with the **United Front Work Department**, with funding provided by foreign nationals located in China and Hong Kong. The UFWD is alleged to be seeking to cultivate relations with influential figures to ensure the UK political landscape is favourable to the CCP.
- Christine Lee was an example of a "seeding operation", reflecting the way the Chinese state operatives are willing to wait years for efforts to pay off. They are prepared to invest in cultivating people at local level potentially and at the outset of their political career.

Slide 15: Cultivation and Elicitation: Senator Feinstein & her driver

- Democrat Senator Dianne Feinstein worked along side a Chinese spy in her San Francisco field office for 20 years. Listed as an "office director" on payroll records, the staffer was her driver, gofer and acted as a liaison to the Asian American community, even attending Chinese Consulate function for the senator. In fact, he reported to China's Ministry of State Security through China's San Francisco Consulate.

- Feinstein acknowledged the infiltration but played down its significance, claiming the staffer never had access to classified or sensitive information or legislative matters. However, it seems improbable that Feinstein never once discussed anything sensitive in her car over the period of years that he worked for her. It is likely that the driver may have had access to conversations in the car or to devices she left in the car while attending functions.
- , while the staffer was fired, no charges were ever filed against him since he was providing political intelligence and not classified intelligence, making prosecution far more difficult.
- Feinstein not only had access to the Chinese community, she had a great amount of political influence and close ties to the intelligence committees.

Slide 16 – Social Media Manipulation (GAC LEAD)

Slide 17 – How to protect yourself? (CSIS LEAD)

- Be discreet, avoid "over-sharing", and assume public conversations are monitored.
- Be aware and keep track of unnatural social interactions, frequent requests to meet privately, out-of-place introductions or engagement, gifts and offers of all expenses paid travel.
- Avoid sharing compromising details or personal information with untrusted individuals, both in-person and online.
- Be aware of inappropriate requests which involve money, and question the source of suspicious donations or "gifts".

Slide 18 – Cyber Threats to Parliamentarians (CSE LEAD)

Slide 19 – How to protect your digital self? (CSE LEAD)

- Be cyber safe. Use strong passwords, enable two-factor authentication, and don't click on links or open attachments unless you are certain of who sent them and why.
- Apply updates to your mobile devices, computers and applications in a timely manner.
- Store your data securely.
- Be wary of connecting devices to unsecured or free Wi-Fi networks
- Be mindful of your online presence.
- Be critical of what you are consuming online, Set up social media and web monitoring, as well as alerting services for identifying and tracking fake news and deep fakes related to your brand and organizations
- Be careful what you share (or repost from others), and take note of unexpected online interactions.
- Follow security of information protocols, don't disclose information to individuals who don't have a reason to access it, and be discrete about how you handle sensitive information.

Slide 20 – How to Report

- There are multiple reporting mechanisms available to report suspected threats of foreign interference. These reports will be dealt with appropriately, while respecting privacy and confidentiality of the individuals reporting the threat.