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 Task Force (SITE-TF) 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. CSIS is currently the Chair of the Security and Intelligence Threats to Elections Task Force (SITE TF).
- SITE TF was established with the mandate to monitor threats to elections. SITE was active in both 2019 and 2021.
- More recently, on PM's direction, SITE has also been mandated to be active during federal by-elections.
- So how does the coordination of the work of the SITE TF members translate into facts?
  - For example, following the SITE TF FI briefing, PCO received a lead from a political party, on one of their candidates being the subject of extortion with a potential foreign interference nexus.
    - [redacted]

- PCO S&I urgently engaged SITE TF members on the case.
- It was determined that the regional police body had the lead on this case as the police of jurisdiction conducting the investigation.
- The next day, SITE members had performed initial checks and determined no indicators of foreign interference at this point.
- PCO then shared further information with SITE, including new messages received by the candidate referencing his MP candidacy;
- SITE TF performed further checks on all available data;
- SITE TF engaged in regular follow-up meetings/updates on the case with PCO to provide them with results and input to support PCO's sound recommendations to the political party to mitigate potential FI activities.

Slide 4 – Toronto-St. Paul's By-Election: Current posture

- Further to PM's direction, the SITE-TF was activated to provide enhanced monitoring to detect any potential foreign interference and violent extremism risks during the Toronto-St. Paul's by-election.
  - Monitoring has started from the beginning of the writ period on May 19th and will continue one week after the election, until June 30th. During this period each of the four Task Force members will align their internal processes to be able to quickly surface, review and forward any reporting of note to the task force;
    - Weekly situational reports and briefings will be provided at classified levels;
    - After action reports will be issued, both at classified and unclassified levels after the election.

Slide 5 – What is foreign interference?

- The SITE TF monitors both FI and domestic terrorism threats to elections.

- The Government of Canada defines **foreign interference** as malign activities undertaken by states, or their proxies, that attempt to **clandestinely or deceptively manipulate** Canada's open democracy and society, 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. We'll cover later FI tactics and techniques
- Foreign interference is distinct from normal **foreign influence** which is a healthy part of diplomatic relations. Foreign Influence include normal diplomatic conduct or acceptable foreign-state actor lobbying.
    - SITE-TF's mandate on foreign interference in elections focusses on ensuring coordinated information sharing, alignment and awareness on foreign interference opportunities targeted by (or subject to) covert, clandestine or criminal activities.

Slide 6 – Risk of Violence/Violent Extremism? (LEAD CSIS/RCMP)

- The Government of Canada defines domestic terrorism in three categories: (i) ideologically motivated violent actors, who are driven by a range of grievances deeply intertwined with conspiracy theories; (ii) religiously motivated violent actors, who encourage violence against perceived immorality; and (iii) politically motivated violent actors who seek to establish new political norms within existing systems through the use of violence. SITE TF monitors these domestic threats in the context of their possible impact on election security, as all these violent actors could possibly target both the public and the government.

(RCMP present their slide)

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 Five 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 – Targets of FI: Elected and Public Officials

- FI activities are persistent, multi-faceted, and target all areas of Canadian society including but not limited to Canada's fundamental institutions (e.g. academia, free press, democratic institutions), governance processes, and diverse Canadian communities.
- 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**.

- 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 9 – What FI 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, officials, 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 10 – Who are the prominent FI actors?

- **People's Republic of China (PRC), China,** using a combination of overt and clandestine means and seeks to exert influence internationally.
    - In Canada, the PRC's FI activities are Party-agnostic and target all levels of processes. The PRC uses a wide range of tools and tactics in a bid to strengthen its pro-China narratives.

- 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.

- **Government of India (GoI), 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.
  - To do so, the GoI can use Canada-based proxy agents and a wide range of FI activities.

- **Russia:** As part of its FI operations, Russia carries out disinformation and propaganda efforts in the West to advance its strategic objectives. Russia is currently not a significant FI actor in Canadian federal elections, but remains a persistent FI threat to Canada. FI tools used by Russia include an established network of pro-Kremlin or opportunistically aligned activists.
  - 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 uncovered 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

- **Government of Pakistan (GoP), Pakistan** seeks to clandestinely influence Canadian Federal politics in order to further GoP's interests in Canada.
  - Pakistani officials in Canada have likely tried to clandestinely influence and support Canadian politicians, at multiple levels of government, with the aim of furthering Pakistani interests in Canada.
  - The Government of Canada (GC) conducted Threat Reduction Measures (TRM) in advance of the 2019 Canadian federal election, to reduce the foreign interference (FI) threat posed by the GoP. These measures included meeting with several individuals and potentially political figures – either candidates or elected officials who have been targeted for foreign interference by the foreign state to discuss the activity of concern.

Slide 11 – Known FI opportunities

1. **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. We have seen political parties and candidates receive donations, seemingly from a Canadian, though actually originating from a foreign threat actor.
    a. For example, prior to and during the 43rd General Election of Canada in 2019, 11 political candidates and 13 political staff members were either implicated in or impacted by a group of known and suspected PRC-related threat actors in Canada
        i. PRC officials met with political staffers and specifically conveyed their expectation for candidates' screening at certain events.
        ii. Some of the PRC-related threat actors received financial support from the PRC, through two transfer of funds- approximating $250,000 from PRC officials in Canada between late 2018 to early 2019. Funds were transferred via multiple individuals to obfuscate their origins
    b. During the 44th General Election in Canada in 2021, the government of India's (GoI) FI activities centered on a small number of electoral districts
        i. Some of the districts were of interest to the GoI owing to the GoI perception that a portion of Indo-Canadian voters

were sympathetic to the Khalistani movement or pro-Pakistan political stances

- GoI proxy agents may have attempted to interfere in democratic processes, including through the clandestine provision of illicit financial support to various Canadian politicians as a means to secure the election of pro-GoI candidates or gain influence over candidates who take office

2. Interference in Nomination Processes

a. Preceding the 43rd General Election of Canada in 2019, irregularities have been noted in the nomination process of the Liberal Party of Canada (LPC) candidate for Don Valley North (DVN). Interference may have included activities undertaken by individuals close to PRC and the involvement of a known proxy agent of PRC Officials

- Buses were used to bring international students to the nomination process, in support of a candidate;
- Students were provided with falsified documents to allow them to vote, despite not being residents of DVN;

3. Influencing community groups

a. In the course of the Greater Vancouver election for the 43rd General Election of Canada in 2019, some PRC officials likely favoured particular political candidates and political parties, and clandestinely leveraged Canadian and Canada-based PRC proxy agents to support the PRC's preferred candidates

- PRC officials clandestinely coordinated the exclusion of candidates, perceived as 'anti-China', from local community events related to the election.
- PRC officials' involvement was obfuscated through the use of PRC proxy agents.

4. Coercive measures

a. Preceding the Don Valley North (DVN) election for the 43rd General Election of Canada in 2019, PRC likely used coercive measure to support the Liberal Party of Canada (LPC) candidate Han Dong
   - Coercive measures included veiled threats issued by the PRC Consulate to the Chinese international students, implying Student visas would be in jeopardy, and consequences for the students' families back in the PRC if students did not support Han Dong.

5. Misinformation / 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.

a. For example, over the course of the 44th General Election of Canada, in late August 2021, CPC leader (Erin O'Tool) was the subject of media misinformation, when an erroneous information-including claims about an intent to ban WeChat-was posted in a York BBS article focused on the CPC's electoral platform

- The inaccurate claims were reprised and spread within Canada's Chinese language media ecosystem. Then PRC state media published an article claiming hostile China blueprint among Canadian Tories. This article was then widely spread within Canada's Chinese language media ecosystem, without attribution to PRC state media.

b. Over the course of the 44th General Election of Canada, in early September 2021, Kenny Chiu, CPC MP and candidate for Steveston-Richmond East in British Columbia, as well as his Bill C-282 to establish the Foreign Influence Registry were the subject of misinformation

- 105.9 Yes My Radio posted an anonymous article containing erroneous information on Mr. Chiu and his Bill C-282, that was shared within Canada's Chinese language media ecosystem. Similar claims were then posted by Global Chinese Convergence Media, adding Mr. Chiu's alleged "anti-PRC" activities.
- The same claims were then repeated in Today's Commercial News posts encouraging people to further share the article within Canada's Chinese language media ecosystem.

6. Social Media Manipulation

(GAC will present examples)

a. Disinformation campaign against Mr.Chong (between May 4 and 13, 2023):

- a coordinated network of WeChat news accounts featured, shared and amplified false or misleading narratives about Mr. Chong' s identity, including commentary and claims about his background, political stances and family heritage.
- GAC judges it highly probable China played a role in the information operation based on indicators such as:
  coordinated content and timing;
  highly suspicious and abnormal shifts in volume and scope of engagement; and
  the concealment of state involvement.

b. Spamouflage (August 2023): Spamouflage is a well studied tactic or technique using networks of spam social media accounts.
   - this activity targeted dozens of MPs from across the political spectrum and included "Deepfake" videos of a Canada based critic of Chinese Communist Party (CCP) criticizing the Prime Minister.- Very low engagement/reach to audiences but observed on multiple western social media platforms. GAC judges it highly probable that it is connected to China based on previous reporting from industry and academia.

c. Indicators to look for: Anonymous networks spreading false narratives, posting at the same or near same time, which then get amplified by state media or officials

Slide 12 – Cyber and Digital Threats to Parliamentarians (CCCS LEAD)

(CCCS/CSE will present)

Slide 13 – How to protect yourself? (joint CSIS/CCCS/CSE LEAD?)

- Be aware and keep track of "unnatural" social interactions.
- Be aware of inappropriate requests that involve money, suspicious donations, free trips, personal benefits, or "gifts."
- Follow protocols on the security of information.
- Be diligent with information sharing and partnerships.
- Practice good password etiquette and use Two-factor identification whenever possible.
- Apply updates to your mobile devices, computers and applications.
- Secure your social media account.
- Be on guard for phishing and spear-phishing messages.
- Store your data securely and know your back-up procedures.
- 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 wary of connecting devices to unsecured or free Wi-Fi networks.

Slide 14 – 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.