UNCLASSIFIED//FOR OFFICIAL USE ONLY

Briefing to Elected Officials on Foreign Interference

How can you protect yourself and your staff?

The primary goal of the below is to make you more resilient to the foreign interference efforts of hostile states that seek to target you. You should be aware that hostile states may seek to target you directly, or via third parties they trust.

1. **Be Aware:** The first and most important step you can take as an elected official is to **be aware** that you are of immediate and constant interest to certain hostile state actors seeking to interfere in Canada's democratic and electoral institutions and processes. These states actively target our elected officials and their staff to achieve several goals, including a) furthering their own national interests in Canada, b) using Canadian officials and staff to 'speak out' on and support topics which are of critical importance to their regimes, and c) silencing critical voices which may raise legitimate concerns about the behaviour of these hostile states. You should also be aware of **how** they target you and their tradecraft – we will get into that shortly.

2. **Elicitation:** Keeping the above in mind, it is important to be aware of attempts at **elicitation**. To further their interests, threat actors will seek to circumvent direct engagement with relevant federal government authorities (e.g. Global Affairs Canada) and directly engage with officials like yourself (as well as their staff) to collect information. Elicitation involves efforts to purposefully provide individuals with limited or incorrect information in the hopes that they will a) provide additional information about an issue of interest, or b) correct the threat actor and provide a proper, previously unknown account of a specific area of interest.

    - **To protect yourself, be aware of attempts by individuals to elicit information from you, and avoid 'over-sharing' whenever possible. You should assume public conversations are monitored.**

3. **Cultivation:** Threat actors can be extremely patient in their interference efforts. Effective threat actors seek to build long-lasting, deep relationships with targeted persons. Often, they will seek to **cultivate** individuals of interest to them over time, sometimes with the provision of 'favours' or via requests for similar favours in exchange. Cultivation begins with a simple introduction, and threat actors utilize innocuous social gatherings and shared interests in an effort to build personal relationships which can be leveraged for interference efforts in the future.

    - **To protect yourself, be aware and keep track of strange social interactions, frequent requests to meet privately, and out-of-place introductions or engagements. Be aware of efforts targeting your staff, and also note odd attempts seeking employment with your office. It is important to also note that sometimes, threat actors will seek to use staff members to interfere in your schedule and set up opportunities for cultivation.**

4. **Blackmail/Threats:** In extreme circumstances, hostile states may seek to use **blackmail and/or threats** to secure cooperation from a specific individual (e.g., to not attend specific events, to not travel to politically sensitive locations, to support a foreign state objective, etc.). Hostile states may threaten to negatively impact your financial/electoral support, even threaten to support an opponent. These threats may come either directly from a hostile state or via trusted third parties. If a threat actor becomes aware of compromising or otherwise embarrassing details regarding your life, they can seek to blackmail you. Sometimes, blackmail or threats may occur after a long period of cultivation and relationship-building. A threat actor may also seek to place you in a compromising situation in an effort to blackmail you later.

    - **To protect yourself, avoid sharing compromising details about your life with untrusted individuals, both in-person and online. Certain states will seek to leverage social media in an effort to build relationships – you should be aware that online personas you engage with may not be who they say they are. Avoid placing yourself in compromising situations, and seek assistance if someone seeks to threaten or blackmail you.**

5. **Illicit Financing**: Threat actors may seek to use you as a proxy to conduct illicit financing on their behalf. Inducements may occur innocuously via a simple request for a favour. For example, a threat actor may ask you to 'pay someone back' or relay money to a third party on their behalf. Political parties and candidates may also receive funds seemingly from a Canadian, though this may have originated from a foreign threat actor.

    - **Be aware of inappropriate requests which involve money, and question the source of strange donations or 'gifts'. Question the origins of spontaneously large donations from unknown individuals who may appear to have linkages to a foreign government and be aware of how fundraising events are structured and operated. Staff members may also be impacted by such activities.**

6. **Cyber Tools**: Your electronic devices can be compromised through a range of **cyber tools and tradecraft.** Socially-engineered e-mails (i.e., 'spear-phishing' emails) can trick you into a clicking a specific link and sharing details about your devices, or can potentially introduce harmful malware into your systems. These cyber tools enable threat actors to collect potentially useful information that can be used in a foreign influence operation (e.g. voter data, compromising information about a candidate).

    - **Practice good digital hygiene. Do not mix personal and professional devices. Use strong passwords, enable two-factor authentication, and do not click on links/open attachments unless you are certain of who sent them and why.**
    - **Do not use untrusted applications or software developed in hostile states with nebulous or problematic legal regimes. If you must use untrusted applications, do so on a 'clean' device which does not contain personal or professional information and**

has limited connectivity to you or your office.

7. **Social Media Manipulation**: Threat actors can manipulate social media to spread disinformation, amplify a particular message, or 'troll' users, when appropriate. By using specific manipulation tactics, threat actors can potentially impact voter opinions and degrade the reputations of elected officials.

    - **Be careful in what you share on-line (or re-post from others); take note of odd online interactions and content. Be aware that hostile states may try to engage with you via 'cut outs' or false personas through social media platforms such as LinkedIn, Twitter, or Facebook. When possible, try to establish the bona fides of individuals you engage with online.**

8. **Lastly**, if you ever feel like you are being targeted by a hostile state or state-linked threat actors, **please contact us**. We are here to help as much as possible, whenever we can.