

BRIEFING TO POLITICAL PARTIES
on
THREATS TO CANADA'S ELECTORAL PROCESS

TALKING POINTS FOR THE ASSISTANT SECRETARY TO CABINET
(MACHINERY OF GOVERNMENT AND DEMOCRATIC INSTITUTIONS)

Friday, 20 August 2021
10:00 AM – 12:00 PM

CONTEXT

- These briefings are taking place in the context of ongoing, broader Government of Canada measures to protect our democratic institutions and processes – and particularly our elections – from interference.
- These measures compose the “Protecting Democracy” (PD) framework that mobilizes expertise from across the Government of Canada
- These efforts are complementary to the work of Elections Canada, which is an independent agency of Parliament tasked with administering elections.

MEASURES TO PROTECT CANADA'S DEMOCRATIC INSTITUTIONS AND PROCESSES

- The PD framework was launched ahead of the 2019 General Election. It remains in place, with its measures having since been renewed and refined following independent and internal assessments.
- Assessments revealed no fundamental flaws or major gaps in existing measures, though ongoing vigilance is required to adapt to threats and learn from the experiences of others.
- The framework is based on four “pillars.” Descriptions of and links to measures are available on DI's website.

Pillar 1: Enhancing Citizen Resilience

- Critical Election Incident Public Protocol (the Protocol)
 - created to establish a clear, impartial & non-partisan process to inform Canadians in the event of an incident « threatening Canada's ability to have a free and fair election » (high threshold).
 - Panel composed of Clerk, NSIA and DMs of Justice, Public Safety and Foreign Affairs; decisions taken by consensus.
 - only in place during Caretaker Convention application period.
 - threshold not met during GE43.

- Protocol was a pilot project to be independently evaluated after GE43, to determine whether it should be renewed and/or modified.
- Following independent assessment (Judd report – full report shared with PM and NSICOP; unclassified version published online in December 2020) some amendments were made (none fundamental):
 - Protocol made permanent (until/unless repealed by Cabinet)
 - Application period aligned with Caretaker Convention
 - Mandate clarified to include both foreign and domestic interference
 - Panel explicitly empowered to consult sources outside the security and intelligence agencies, including Chief Electoral Officer
 - Political parties empowered to report election-related interference (via contacts provided at political party briefings)
- **Important note:** *the Protocol provides for the leaders of parties represented in the HoC (or security-cleared designates) to be notified ahead of an announcement. were sent to parties requesting contact information for the leader/designate to receive an invitation to a pre-announcement briefing, if required. As of Thursday, responses were received from the Conservatives, NDP and Bloc.*
- Digital Citizen Initiative: digital, news and civic literacy funding for civil society to support citizen resilience against disinformation.
- 2021 update to CSE's 2017 and 2019 reports on Cyber Threats to Canada's Democratic Process (released July 2021).
- CSIS public report on Foreign Interference Threats to Canada's Democratic Process (released July 2021)
- Get Cyber Safe campaign: national public awareness campaign to educate Canadians about cyber security

Pillar 2: Improving Organizational Readiness

- Classified briefings to political parties
- Cybersecurity guidance to political parties
- Cybersecurity hotline to report cyber incidents
- Engagement with Elections Canada

Pillar 3: Combatting Foreign Interference

- Security and Intelligence Threats to Intelligence Task Force (SITE): CSE, CSIS, RCMP, GAC and PCO coordination to “prevent covert, clandestine, or criminal activities from influencing or interfering with the electoral process in Canada.”

- G7 Rapid Response Mechanism: created under Canadian leadership following 2018 G7 Summit to “manage, triage, share information and identify opportunities for a joint G7 response to threats to democratic processes.” This is done through social media analytics & information-sharing.

Pillar 4: Supporting a Healthy Information Ecosystem (formerly Expecting Social Media Platforms to Act)

The Canada Declaration on Electoral Integrity Online - What and Why

- Democracies around the world are all struggling with the challenges of addressing disinformation and other potential harms circulated on social media, while maintaining and safeguarding citizens’ freedom of expression.
- In 2019, we decided that one way to protect this freedom was a voluntary code with the key Internet companies on whose platform Canadians debated and deliberated their electoral options and futures.
- This voluntary code, The Canada Declaration on Electoral Integrity Online (the Declaration), outlines commitments for both industry and government, around three key principles: Integrity, Transparency and Authenticity. This reflects that both government and industry have a role to play in upholding these principles.

Renewed Declaration and Changes

- In August 2021, key social media platforms operating in Canada acknowledged the renewal of an updated Canada Declaration on Electoral Integrity Online. Facebook, Google, LinkedIn, Microsoft, TikTok, Twitter and YouTube endorsed the renewed Declaration.
- The first commitment in the Declaration is for platforms to “Intensify efforts to combat disinformation that poses a threat to Canada’s democratic processes and institutions”.

Examples of Actions by Social Media Companies

- In July 2021, two notable reports were published on the threats to Canada’s democracy. The Canadian Security Intelligence Service published Foreign Interference Threats to Canada’s Democratic Process, wherein, the Service

notes it has observed “social media being leveraged to spread disinformation or run foreign influenced campaigns designed to confused or divide public opinion, or interfere in healthy public debate”.

- However, in their Cyber Threats to Canada’s Democratic Process: July 2021 update, the Communications Security Establishment points to the “efforts by social media companies to identify and remove accounts engaging in coordinated inauthentic behaviour online as well as flagging problematic content” as one the important countervailing trends to cyber threats to democracy.
- There are a variety of ways that companies will take action against disinformation on their platforms. Most companies will have standard content policies which apply irrespective of an election period (for example: some companies will forbid the use of automated accounts to manipulate the platform and will remove millions of accounts before they are ever noticed and/or reported by users.
- Companies have also introduced a number of specific policies related to disinformation. For example:
 - Facebook has expanded its fact-checking partnerships in Canada and introduced new requirements for Pages to be labeled as “News” organizations.
 - Although Facebook’s community standards forbid posting misleading information around how or when to vote, during the election, the company will combine human and automated review and proactively seek out such potentially misleading content to remove it form the platform.
 - TikTok forbids the spread of disinformation on its platform, the impersonation of others, and the use of automated accounts to generate fake engagement. The company has also committed to working with fact-checking partners.

- Twitter’s civic integrity policy forbids using the platform “for the purpose of manipulating or interfering in elections or other civic processes”. In this policy the company commits to labelling and reducing the visibility of Tweets containing false or misleading information about civic processes.
- The renewed Declaration includes a commitment by companies to publicly post the actions that they are taking in support of the Declaration and to protect election integrity, and I encourage you to visit the platform links that are posted on the Government of Canada, Democratic Institution Protecting Democracy website.

CONCLUSION

- PD framework is robust, and GoC is ready to act in the event of interference in our democratic processes – and particularly the election.
- GoC remains attentive to developments both at home and abroad in order to refine measures as required.
- Look forward to continuing to work together to protect our democratic process.