Protected B

Deputy Ministers' Cyber Security Committee
October 30, 2023 – 10:00 AM to 11:30 AM
PCO Secure Mobile (CISCO)
(1.5 hours)

ANNOTATED AGENDA

ITEM #	INFORMATION
1.	**OPENING REMARKS** *(10 min)* • PS - Shawn Tupper, Deputy Minister PS • CSE - Caroline Xavier, Chief CSE DMCS meeting agenda available at **Tab A**.
2.	**OPERATIONS UPDATE** *(20 min)* **Objective**: *CSE, RCMP, and CSIS to share information on latest operational issues.*
3.	**THREATS TO DEMOCRATIC PROCESS REPORT #4** *(20 min)* **Objective:** *CSE to provide overview of the report to be released.* **Deck (Tab B), Summary** • *Cyber Threats to Canada's Democratic Process* is a public report issued by CSE's Centre for Cyber Security every two years since 2019 which explores global trends in threat activities against democratic processes and assesses implications for Canada. The last report was released in 2021. • The 2023 report notes the following 4 trends: 1. Targeting of democratic processes has increased 2. Russia and China continue to conduct most of the attributed cyber threat activity targeting foreign elections 3. The majority of cyber threat activity targeting elections is unattributed. 4. Online disinformation is now ubiquitous in elections globally and generative artificial intelligence is increasingly used by adversaries to influence elections. *Continued on next page…*

[APG] / [ANP]

3. cont.

Threats to Democratic Processes Report #4, Continued

- While a draft is not yet available, CSE notes that the report will convey key implications for Canada:
  - Disinformation (including from deepfakes and social botnets) will likely be used to target Canada's elections in the next two years.
  - Elections systems and online information ecosystems and are likely to be targeted more than they have been in the past, particularly by state actors with which Canada has bilateral tensions (China, Russia,
  - Attribution of cyber incidents will become increasingly difficult.
  - Moving to completely digital with ballots presents risks to election integrity.

- Cyber Centre is proposing a high-profile communications approach for the release of the report, with Chief CSE as lead spokesperson, and media and stakeholder briefings.

PCO Comment

- PCO S&I, IAS, Democratic Institutions and Communications have not yet been consulted on the report nor the communications strategy.

- PCO notes that the proliferation of generative AI tools will empower ***all*** potential threat actors (not only China/Russia) to create and spread disinformation as it grants capacity to individuals even with limited resources.

- PCO notes that identifying mis/dis-information on social media increasingly important to election security. The RRM conducts the activity at a small scale, but a larger-scale approach will be needed to address the increased threat.

Suggested Interventions:

- **You may wish to convey that PCO has no concerns with the conclusions of the report - it will be an important tool for explaining and contextualizing cyber threats to our democratic systems – particularly as we navigate the Public Inquiry on Foreign Interference.**

Continued on next page…

- **You may wish to request that DMs have a chance to review the full report prior to its publication – especially given CSE indicates there are statements related to**

3. cont.	○ Particularly when it comes to democratic institutions and elections security, we have to be coordinated – both in our assessments but also our processes and communications. • **You may wish to express that, PCO would support a proactive communications strategy in consultation with PCO Comms.** • **You may wish to note that the findings of the report highlight the need for even more coordination among members of the intelligence community and the need to address gaps – including our ability to address the growing threat of mis/dis-information.**
4. 4. cont.	s. 39 - Cabinet Confidence

2. National Cyber Security Strategy

- The National Cyber Security Strategy was last discussed by DMs at the August 22, 2023 DM Cyber.

s. 39 - Cabinet Confidence

3. TBS Government of Canada Enterprise Cyber Security Strategy

- TBS is developing the GC Enterprise Cyber Security Strategy in response to direction from a Budget 2022 off-cycle FES decision.
- TBS sought DM endorsement of the strategy at the August 22, 2023 DMCS meeting. s. 39 - Cabinet Confidence

s. 39 - Cabinet Confidence

s. 39 - Cabinet Confidence

Continued on next page…

4. cont.

- **You may wish to convey to PS and partners contributing to the Cyber Strategy renewal that a long-term strategy does not need to move forward with immediate funding. Funding for specific initiatives can be sought in future years.**
- **You may wish to note that the strategy should be about how we approach cyber security. While new funding would help address gaps, if we can't afford new initiatives, we need to be creative about how we use the programs and skills we have. The Cyber Strategy was set to be renewed in 2022 – we can't wait until the fiscal situation improves.**

	s. 39 - Cabinet Confidence

5.	**FORWARD AGENDA** *(15 min)*
	
	Objective: *PS and CSE to lead discussion on priority items for the committee.*
	
	• Documents included at **Tab C**.
	
	Suggested Interventions:
	
	BGRS Cyber Incident
	• **You may wish to invite the DMCS co-chairs to consider adding a discussion on the lessons learned from the BGRS incident to the forward agenda.**
	  ○ The BGRS incident highlights challenges when a supplier to the GC is impacted by a cyber incident. In this case, since BGRS is not critical infrastructure, falls outside of the Federal Cyber Incident Response Plan and Government of Canada Cyber Security Emergency Plan. DMs may wish to discuss how to best address incidents of this nature in the future.
	  ○ ADMs continue to develop interim measures to address the current incident.

6.	(All) **ROUNDTABLE AND CLOSING REMARKS** *(10 min)* **Suggested Interventions**: s. 39 - Cabinet Confidence