

**PUBLIC INQUIRY INTO FOREIGN INTERFERENCE  
IN FEDERAL ELECTORAL PROCESSES AND DEMOCRATIC INSTITUTIONS**

---

**THE GOVERNMENT OF CANADA'S UNCLASSIFIED WRITTEN SUBMISSIONS  
(PART C HEARINGS)**

---

November 4, 2024

**ATTORNEY GENERAL OF CANADA**

Department of Justice Canada  
Civil Litigation Section  
50 O'Connor Street, Suite 500  
Ottawa, Ontario, K1A 0H8  
Fax: (613) 954-1920

**Gregory Tzemenakis**

Senior General Counsel

**Barney Brucker**

A/Senior General Counsel

**Tel:** 613-297-2670 / 416-520-4301

**Email:** [JusticeCanada.Inquiry-Enquete@iustice.gc.ca](mailto:JusticeCanada.Inquiry-Enquete@iustice.gc.ca)

**Counsel for the Government of Canada**

## Table of Contents

A. Overview.....	1
B. Foreign Interference in Canada.....	1
C. Canada’s Response to Foreign Interference.....	4
1. Strengthening Canada’s Electoral System .....	6
a) Panel/CEIPP.....	6
b) SITE TF .....	7
2. Collaboration With Parliamentarians, Political Parties and Other Governments .....	9
a) Canada has made the Political System more Resilient .....	9
b) Canada has Partnered with Other Levels of Government.....	13
c) Canada Coordinates with International Partners.....	14
3. Canada is Building Public Resiliency to FI .....	15
a) Collaboration with Cultural Communities.....	16
b) Working with civil society organizations to build resilience .....	17
4. Canada’s National Security Community has the Capacity to Detect, Deter and .....	
Counter FI .....	20
a) CSIS - Intelligence Tools .....	21
b) CSE – Foreign Signals and Cyber Defence Tools .....	22
c) GAC - Diplomatic Tools .....	23
d) RCMP - Law Enforcement Tools.....	26
e) Public Safety - Regulatory Tools .....	27
5. The Government’s Response to FI Threats is Coordinated .....	27
a) National Security Council (NSC) .....	27
b) Deputy Minister Coordination .....	28
c) National Counter Foreign Interference Coordinator.....	29
d) Intelligence Dissemination.....	29
D. Canada’s Response to Specific Incidents and Allegations.....	32
1. Political Party Processes are the Domain of Political Parties .....	32
2. Public Service Debate about FI is a Strength, not a Weakness.....	32
3. Overseas Police Stations .....	33

- 4. Targeting Paper and Special Report not being provided to the PM..... 34
- 5. CSIS warrants and the timeline for one to be approved ..... 34
- 6. Hostile Activities by State Actors (HASA) Memorandum to Cabinet and Bill C-70..... 36
- E. Canadians Can and Should have Confidence ..... 36
  - 1. Confidence in 43<sup>rd</sup> and 44<sup>th</sup> General Elections ..... 36
  - 2. Confidence in Democratic Processes..... 37
    - a) Media reporting on FI in late 2022 and early 2023 ..... 37
  - 3. Confidence in Parliamentarians ..... 38
- F. Conclusion ..... 39

## **A. Overview**

1. For almost a decade, the Government of Canada has worked resolutely across many fields to fortify Canada's capacity to detect, deter, and counter foreign interference (FI). It has better equipped the electoral and broader political system; led action on the international stage; further strengthened the national security and intelligence community; and built up the resilience of the public.
2. Contrary to the incorrect picture painted by media stories based on illegal and misleading leaks, the evidence heard by this Commission shows that Canadians can and should have confidence in the integrity of their democratic institutions, including their elections, their government, and the Parliamentarians who represent them. Despite malign and unacceptable FI activities, those institutions were and continue to be fundamentally sound.
3. The government's long and broad track record of strong action does not mean that FI is a solved problem. FI is carried out in a shifting geopolitical context, by states that will continually change their tactics to try and circumvent Canada's defences. FI actors exploit Canada's freedoms by taking advantage of the openness of the internet to spread disinformation and by victimizing certain communities through the links they maintain with their countries of origin. FI often occurs through the expressive and participatory rights that are fundamental to our democracy.
4. For these reasons, FI is, by its nature, a complex, challenging, and evolving problem. It remains a threat that must be countered with focused action and a sense of urgency. Government's work must and will continue. The Commission's recommendations will influence that future work, in addition to its critical role in contributing directly to the public's understanding of the FI threat. Canada thanks the Commission for its careful study.

## **B. Foreign Interference in Canada**

5. To detect, deter and counter FI, it is crucial to understand the threat. FI is complex and evolving. A threat faced by all democracies, FI activities can take many forms, target many parts of society, and employ diverse methods. Canada continues to develop a sophisticated

understanding of FI, the tactics and objectives of hostile state actors, and the different vectors and methods that can be employed.

6. FI is not new. Countries have long sought to influence each other's policies, and that is the business of diplomacy, rooted in the *Vienna Convention on Diplomatic Relations* and the *Vienna Convention on Consular Relations*.<sup>1</sup> Foreign influence becomes FI when it is covert, clandestine or involves threats to individuals.<sup>2</sup> It can sometimes be hard to determine whether specific activity is FI or foreign influence.<sup>3</sup> FI is especially pernicious when it attempts to undermine Canadian democracy, values or objectives. FI actors may intentionally operate in a manner to obfuscate their FI activities.

7. In Canada, the People's Republic of China (PRC) and India currently represent the most pervasive and active FI threats. Russia and Pakistan also attempt forms of electoral FI. Other countries, including the notable example of Iran, do not directly target Canada's democratic institutions, but nevertheless undertake other forms of FI, including transnational repression (TNR).<sup>4</sup>

8. As the Commission noted in its Initial Report, FI activities are not just about elections, nor even just about democratic institutions.<sup>5</sup> The Commission's mandate is broader than just elections but is limited to electoral processes and democratic institutions. Although Canada is responding to FI activities across a much broader spectrum, these submissions address only those activities and responses that are within the mandate of the Commission.

---

<sup>1</sup> Global Affairs Canada, Public Hearing Transcript, [Volume 10](#), pp 9-17.

<sup>2</sup> Global Affairs Canada, Public Hearing Transcript, [Volume 10](#), p 18.

<sup>3</sup> Global Affairs Canada, Public Hearing Transcript, [Volume 10](#), pp 18-20.

<sup>4</sup> Country Summaries, [CAN.SUM.000030](#); *In Camera* Examination Summary: CSIS SITE Representative #1, CSIS SITE Representative #2, Ryan Macdonald, Robin Wettlaufer, Greg O'Hayon, [WIT0000139](#), paras 7-12.

<sup>5</sup> Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions Initial Report ("[Initial Report](#)"), p 83.

9. Some activities targeting electoral processes or democratic institutions that have been identified in intelligence reporting include:

- a. illicit efforts to support electoral candidates viewed as sympathetic to or vulnerable to influence by a foreign country's interests;<sup>6</sup>
- b. suppression of electoral candidates or elected officials viewed as antithetical to a foreign country's interests;<sup>7</sup>
- c. suppression of electoral candidate participation in community and election-related events;<sup>8</sup>
- d. implicit or explicit threats against or support to members of cultural communities in Canada;<sup>9</sup> and,
- e. information manipulation in all its forms, including disinformation campaigns on online platforms used by cultural communities.<sup>10</sup>

10. FI targeting democratic institutions manifests itself in two major ways: person-to-person FI and information manipulation. Person-to-person FI includes attempts to covertly influence, intimidate, manipulate, interfere, corrupt or discredit individuals to further the interests of a foreign country. These relationships are often nurtured over an extended period of time.<sup>11</sup>

11. Online information manipulation is a real and present threat to democracies around the world; this will continue to be a matter of concern and priority in the ongoing efforts to counter FI. Democracies have long grappled with the challenges of disinformation and propaganda<sup>12</sup> and the advent of the internet and social media has made new tactics and greater reach possible for hostile state actors. Artificial Intelligence (AI) and the increasing sophistication of hostile online actors make disinformation harder to detect;<sup>13</sup> permissive monitoring and enforcement efforts by

---

<sup>6</sup> Don Valley North, [CAN.SUM.000001](#); People's Republic of China Officials - Foreign Interference Activities in Greater Vancouver in the 2019 General Election, [CAN.SUM.000003](#); People's Republic of China – Threat Actors, Contact with Candidates and Staff, and Funding of Threat Actors, [CAN.SUM.000010](#); Government of India Foreign Interference Activities in the 2021 General Election, [CAN.SUM.000012](#).

<sup>7</sup> People's Republic of China Officials - Foreign Interference Activities in Greater Vancouver in the 2019 General Election, [CAN.SUM.000003](#); PRC Interest in Michael Chong, [CAN.SUM.000017](#); PRC Email Operations Against Parliamentarians, [CAN.SUM.000027](#); Suspected Instances of Foreign Interference, CAN.SUM.000031. \*document unavailable on Commission website

<sup>8</sup> People's Republic of China Officials - Foreign Interference Activities in Greater Vancouver in the 2019 General Election, [CAN.SUM.000003](#).

<sup>9</sup> People's Republic of China Police Stations, [CAN.SUM.000015](#).

<sup>10</sup> The People's Republic of China's Targeting of Parliamentarians for the Purpose of Exerting Influence, [CAN.SUM.000018](#), para 8.

<sup>11</sup> *In Camera* Examination Summary: A Branch within CSIS ADR Directorate, [WIT0000043](#), para 10

<sup>12</sup> Privy Council Office, Public Hearing Transcript, [Volume 29](#), p 54.

<sup>13</sup> The Media Ecosystem Observatory, Public Hearing Transcript, [Volume 22](#), pp 41-42.

private social media companies make it harder to deter;<sup>14</sup> and increasingly segregated groups on social media make it harder to counter.<sup>15</sup> The accelerating decline of traditional news media has amplified these problems.<sup>16</sup>

12. In addition to the foregoing, TNR encompasses efforts by hostile states to harass, intimidate, and coerce people into behaving in certain ways.<sup>17</sup> TNR is broader than FI targeting democratic institutions. The Commission heard courageous testimony from diverse community representatives on the threat and reality of TNR.<sup>18</sup> TNR is unacceptable in Canada and is widely condemned by like-minded countries. Canada is committed to combatting this critical threat and working with cultural communities to build resilience to it.<sup>19</sup>

### **C. Canada's Response to Foreign Interference**

13. Over the last decade, Canada has responded proactively and effectively to the rapidly evolving threat of FI. It has developed innovative responses to the kinds of FI activities seen in Canada and around the world. The result of these ongoing efforts is a more sophisticated technological and human ability to detect, deter and counter FI.

14. Canada must continue to act in a coordinated manner across government and together with other actors in society. This includes the efforts of elected officials and their staff, political parties, cultural communities, civil society organizations, academic institutions, multilateral international organizations and more. As experts noted during the policy hearings, the key to minimizing this threat is to foster continued public trust in democratic processes and in society, which is a complex challenge demanding a whole of society approach rather than something that can be addressed by ad hoc legislative or policy changes.<sup>20</sup>

---

<sup>14</sup> Minister St-Onge, Public Hearing Transcript, [Volume 33](#), pp [115-116](#); The Media Ecosystem Observatory, Public Hearing Transcript, [Volume 22](#), pp [43-44](#).

<sup>15</sup> The Media Ecosystem Observatory, Public Hearing Transcript, [Volume 22](#), pp [30-32](#).

<sup>16</sup> The Media Ecosystem Observatory, Public Hearing Transcript, [Volume 22](#), pp [8-10](#).

<sup>17</sup> [Initial Report](#), pp [87](#), [147](#).

<sup>18</sup> Consultation Panels, Public Hearing Transcript, [Volume 26](#).

<sup>19</sup> Royal Canadian Mounted Police, Public Hearing Transcript, [Volume 27](#), pp [20-21](#).

<sup>20</sup> Policy Roundtables, Public Hearing Transcript, [Volume 36](#), pp [134-135](#).

15. Canada's response to FI requires both urgency and adaptability as the threat tactics evolve. No single response is a panacea. All aspects of government and society must collaborate to respond to this threat.<sup>21</sup>

16. Canada has invested significant resources in developing its ability to detect, deter and counter FI in electoral processes and democratic institutions. In addition to the investments up to 2021 explained in the Commission's stage one investigation, Canada has invested:

- a. \$10 million over five years in the Protecting Democracy Unit at the Privy Council Office (PCO);<sup>22</sup>
- b. \$13.4 million over five years for the ongoing Rapid Response Mechanism (RRM) Canada efforts at Global Affairs Canada (GAC);<sup>23</sup>
- c. \$13.5 million over five years for the National Counter Foreign Interference Coordinator at Public Safety Canada;<sup>24</sup>
- d. \$48.9 million over three years allocated to the Royal Canadian Mounted Police (RCMP) to help counter hostile activities of state actors;<sup>25</sup>
- e. \$31 million over four years to Heritage Canada for the Digital Citizen Contribution Program to help build citizen resilience;<sup>26</sup>
- f. \$917.4 million over five years and \$145.8 million per year ongoing for the Communications Security Establishment (CSE) and GAC to enhance their intelligence and cyber operations programs to respond to evolving national security threats<sup>27</sup>; and
- g. over \$655.7 million over eight years for the Canadian Security Intelligence Service (CSIS) to enhance its intelligence capabilities, keep pace with technological developments and improve its capability to detect, deter and counter FI.<sup>28</sup>

17. Some of the measures currently in place to detect, deter and counter FI in electoral processes and democratic institutions are: 1) structural tools to monitor and defend electoral processes; 2) collaboration with Parliamentarians, political parties and other governments; 3) public information resources and other means of developing public resilience to FI, particularly

---

<sup>21</sup> Minister LeBlanc, Public Hearing Transcript, [Volume 34](#), pp [203-205](#); Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), pp [85-86](#).

<sup>22</sup> Privy Council Office, Stage 2 Institutional Report, [Can.Doc.000036](#), p [8](#).

<sup>23</sup> Global Affairs Canada, Stage 2 Institutional Report, [Can.Doc.000030](#), p [4](#).

<sup>24</sup> Government of Canada provides update on recommendations to combat foreign interference, [COM0000609](#) at p [6](#); Public Safety Canada, Public Hearing Transcript, [Volume 30](#), p [92](#).

<sup>25</sup> Interview Summary: Royal Canadian Mounted Police (Commissioner Michael Duheme and Deputy Commissioner, Federal Policing, Mark Flynn), [WIT0000108](#), para [29](#).

<sup>26</sup> Canadian Heritage, Institutional Report, [CAN.DOC.000034](#), p [2](#).

<sup>27</sup> Communications Security Establishment, Stage 2 Institutional Report, [CAN.DOC.000028](#), p [6](#).

<sup>28</sup> Canadian Security Intelligence Service, Stage 2 Institutional Report, [CAN.DOC.000044](#), p [9](#).



in cultural communities; 4) enhanced tools for the national security agencies; and 5) inter-agency and governance coordination within government. Each is addressed in the following sections.

## **1. Strengthening Canada's Electoral System**

18. As this Commission heard in its first stage, Canada announced the Plan to Protect Democracy in 2019, which includes measures to strengthen our electoral system. The Plan was built around four pillars: a) enhancing citizen preparedness; b) improving organizational readiness; c) combatting FI; and d) building a healthy information ecosystem.<sup>29</sup> Key components of the Plan to Protect Democracy include the Panel of 5 (Panel) and the Security and Intelligence Threats to Elections Taskforce (SITE TF), both of which were discussed in detail in the first stage.

19. New measures have been put in place since the 2021 general election and others are being developed, including a new iteration of the Plan to Protect Democracy.<sup>30</sup> The intention is to implement any measures that are ready in advance of the next general election.

### *a) Panel/CEIPP*

20. As was discussed extensively during the first stage, the Critical Election Incident Public Protocol (CEIPP) established the Panel, empowering experienced senior, objective and non-partisan public servants to monitor general elections daily and to coordinate Canada's response to suspected FI activities during the Caretaker period.<sup>31</sup>

21. The Panel continues to examine and refine its approach. Notably, the Panel monitors elections in other jurisdictions to keep current on best practices. The Panel is ready to respond using different approaches depending on the type of FI that presents itself.<sup>32</sup> The Panel is also working to implement a new communication strategy that would make it better known before, during and after the election,<sup>33</sup> explain its role, and foster Canadians' trust. The first time the

---

<sup>29</sup> Privy Council Office, Public Hearing Transcript, [Volume 11](#), pp 5-11.

<sup>30</sup> Privy Council Office, Public Hearing Transcript, [Volume 23](#), p 120.

<sup>31</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 63-64.

<sup>32</sup> *In Camera* Examination Summary: John Hannaford and Nathalie G. Drouin, [WIT0000150](#), para 8.

<sup>33</sup> *In Camera* Examination Summary: Allen Sutherland, Assistant Secretary to the Cabinet, Democratic Institutions and Machinery of Government, [WIT0000123](#), para 40.

public learns about the Panel should not be when there is an incident that threatens the integrity of an election.<sup>34</sup>

22. The Panel is actively preparing well in advance of the next general elections.<sup>35</sup> New members have received introductory briefings<sup>36</sup> and briefings from the SITE TF on the current threat landscape.<sup>37</sup> The Panel has also met with representatives from civil society, and with representatives from allied countries, to learn from their experiences of electoral FI.<sup>38</sup>

23. To prepare for its role during the Caretaker period, the Panel has undertaken significant work to develop responses to various scenarios, including incidents that fall short of the high threshold of a serious threat to the integrity of an election. The government must be careful not to take on the role of arbiter of the truth or intervene in legitimate democratic discourse, while also ensuring that Canadians know when something of significant concern is observed.<sup>39</sup> The Panel must also take care not to amplify disinformation inadvertently when taking steps to raise the public's awareness.

24. There is no need to fundamentally alter the composition of the Panel. These senior leaders have extensive experience, skill and acumen in their respective domains and are well-practiced in non-partisan decision-making. They share expert knowledge of national security, human rights and FI. Additionally, they can exercise broad authorities to respond quickly to threats, including those that fall below the Panel threshold.

*b) SITE TF*

25. As was discussed in detail in the stage one investigation, the SITE TF is a group of experts from CSE, CSIS, GAC and the RCMP which coordinates the government's intelligence

---

<sup>34</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 64-65.

<sup>35</sup> *In Camera* Examination Summary: Allen Sutherland, Assistant Secretary to the Cabinet, Democratic Institutions and Machinery of Government, [WIT0000123](#), para 40.

<sup>36</sup> Department of Justice Canada, Public Hearing Transcript, [Volume 23](#), pp 219-220.

<sup>37</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 61-62.

<sup>38</sup> Privy Council Office, Public Hearing Transcript, [Volume 23](#), pp 148-149; Department of Justice Canada, Public Hearing Transcript, [Volume 23](#), pp 221-223.

<sup>39</sup> *In Camera* Examination Summary: Allen Sutherland, Assistant Secretary to the Cabinet, Democratic Institutions and Machinery of Government, [WIT0000123](#), para 42.

and information collection and analysis efforts relating to threats to federal elections. Each member works within its respective authority to monitor and address threats to elections.<sup>40</sup>

26. The Prime Minister activated the SITE TF for twelve by-elections in 2023 and 2024, and for future by-elections. More frequent operation has increased group cohesion and has permitted members to test new practices, such as a scenario exercise involving generative AI.<sup>41</sup>

27. During by-elections, the Caretaker period is not in effect and the Panel is not activated. Rather, during by-elections, the SITE TF reports to the Deputy Minister Committee for Intelligence Response (DMCIR), instead of to the Panel. DMCIR is a committee chaired by the National Security and Intelligence Advisor to the Prime Minister (NSIA), which convenes Deputy Ministers from the national security community, the Deputy Secretary to the Cabinet responsible for Democratic Institutions and others. It meets regularly to discuss operational and tactical intelligence requiring a timely response.<sup>42</sup> That committee would have informed the responsible Ministers and invoked the mandates of their own agencies had they observed FI.<sup>43</sup> The SITE TF also provided a classified report after each by-election to the Prime Minister, the Ministers to whom the member agencies report, as well as the Chairs of the National Security and Intelligence Committee of Parliamentarians (NSICOP) and the National Security and Intelligence Review Agency (NSIRA).<sup>44</sup> For increased transparency, the SITE TF also published unclassified reports after the by-elections to inform the public of their findings.<sup>45</sup> This approach was adopted to reassure Canadians that the by-elections were free and fair, and to normalize the role of the SITE TF.<sup>46</sup>

---

<sup>40</sup> Public Interview Summary: Mr. Lyall King, Ms. Tara Denham, Ms. Gallit Dobner, Mr. Eric Gordon, CSIS Representative, [WIT0000045](#), paras [1](#), [10-15](#).

<sup>41</sup> *In Camera* Examination Summary: CSIS SITE Representative #1, CSIS SITE Representative #2, Ryan Macdonald, Robin Wettlaufer, Greg O’Hayon, [WIT0000139](#), para [16](#).

<sup>42</sup> Privy Council Office, Stage 2 Institutional Report, [CAN.DOC.000036](#), pp [25-26](#).

<sup>43</sup> Security and Intelligence Threats Task Force and the 19 June 2023 Federal By-Elections, [CAN031449](#).

<sup>44</sup> Threats to the Canadian Federal By-Elections – June 2023 After Action Report, CAN021929 and Final Reports on Foreign Interference in the June 2023 By-Elections, CAN032238. \*documents unavailable on Commission website

<sup>45</sup> Security and Intelligence Threats to Elections Task Force – Threats to the Canadian Federal By-Elections June 2023, [COM0000606.EN](#).

<sup>46</sup> *In Camera* Examination Summary: Allen Sutherland, Assistant Secretary to the Cabinet, Democratic Institutions, and Machinery of Government, [WIT0000123](#), para [47](#).

28. The role and importance of the SITE TF in monitoring electoral processes is clear. Activating it permanently is under consideration, but no decision will be made before the final report of this Commission has been received, as there are both benefits and disadvantages to doing so.<sup>47</sup>

## **2. Collaboration With Parliamentarians, Political Parties and Other Governments**

### *a) Canada has made the Political System more Resilient*

29. Canada recognizes that a crucial component of its response to FI in democratic institutions is to build the resilience of Parliamentarians. Members of Parliament (MPs) and Senators can be, and have been, targets of FI because of their positions.<sup>48</sup>

30. Canada informs Parliamentarians about the risks of FI through general security briefings, defensive briefings, Threat Reduction Measures (TRMs), unclassified briefings to political parties and classified briefings to security-cleared leaders of recognized political parties in the House of Commons. This is in addition to security briefings, cybersecurity training, and pre-travel briefings provided by the House of Commons<sup>49</sup> and the Senate,<sup>50</sup> which have the responsibility and accountability to educate and protect their Members from FI.

#### i. General Security Briefings for Parliamentarians

31. Canada has long conducted general security briefings for new Parliamentarians, Ministers, and their staff,<sup>51</sup> to inform them of security and intelligence matters, including FI. Canada has also recently started to conduct “refresher” briefings for Ministers’ offices.<sup>52</sup>

---

<sup>47</sup> *In Camera* Examination Summary: The Honourable Dominic LeBlanc, [WIT0000162](#), para 16.

<sup>48</sup> Targeting of Parliamentarians, [CAN.SUM.000018](#), para 3.

<sup>49</sup> Institutional Report of the House of Commons Administration, [HOC0000001](#), pp 8-13;

<sup>50</sup> Interview Summary: Senate Administration (David Vatcher, Julie Lacroix and Shaila Anwar), [WIT0000126](#), paras 15, 20 & 21

<sup>51</sup> *In Camera* Examination Summary: Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald, [WIT0000143](#), p 2.

<sup>52</sup> *In Camera* Examination Summary: Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald, [WIT0000143](#), p 8.

ii. December 18, 2020 letter to all Parliamentarians

32. Former Public Safety Minister Blair sent a letter to all Parliamentarians on December 18, 2020, to educate MPs about FI risks and the avenues for MPs should they have concerns.<sup>53</sup> It was necessary to inform both MPs and Canadians of the nature of the threat, the risk it represented, and how they could respond.<sup>54</sup>

iii. Ministerial Direction on Threats to MPs

33. In 2023, former Public Safety Minister Mendicino issued the *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians* (Ministerial Direction). It directed CSIS to seek, wherever possible, to ensure that Parliamentarians are informed of threats to the security of Canada directed at them.<sup>55</sup> The Ministerial Direction has since been supplemented with a Governance Protocol which details exactly how the Ministerial Direction will be implemented.<sup>56</sup>

iv. Defensive Briefings and TRMs

34. Beginning as early as 2018, CSIS has provided defensive briefings to over 70 MPs to increase their and their staff's awareness of and resilience to FI, and to explain the overall threat they may face by virtue of their position as an elected official.<sup>57</sup>

35. In addition to defensive briefings, CSIS has used its TRM authority to brief MPs who have been the target of FI.<sup>58</sup> Subject to the requirement for a warrant in certain cases, CSIS' TRM authorities can be used when there are reasonable grounds to believe that there is a national security threat and that the TRM action can reduce it. TRMs can be understood generally in three categories of activity: messaging, where information is pushed to a subject in an attempt to influence their behaviour; leveraging, by which a third party is briefed in order to allow the third

---

<sup>53</sup> Letter from Public Safety Minister, [CAN003326](#).

<sup>54</sup> Minister Blair, Public Hearing Transcript, [Volume 33](#), p 73.

<sup>55</sup> Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians, [CAN021931](#).

<sup>56</sup> Implementation of Ministerial Direction to the Canadian Security Intelligence Service on Threats to Parliament and Parliamentarians, [CAN021638\\_0001](#).

<sup>57</sup> Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 10](#), pp [255-256](#) and [258-259](#).

<sup>58</sup> Members of Parliament Chong, O'Toole, Kwan and Chiu were briefed by CSIS pursuant to its TRM authority.

party to use their own authorities to impede a subject from engaging in threat-related activities; and, interference, by which CSIS officials directly affect the ability of the subject to do something.<sup>59</sup> CSIS has undertaken nine non-warranted TRMs related to FI in democratic institutions and processes between January 2019 and the present.<sup>60</sup> While TRMs may allow CSIS to share certain classified information to enable third parties to take action against identified threat-related activities, CSIS must consider the risks of doing so. Sharing classified information with an individual who has not been security cleared, and who is under no obligation to keep the information confidential, may entail a risk of grave injury to national security.<sup>61</sup>

36. In 2023, CSIS used its TRM authorities to brief MPs Chong, Chiu, Kwan, and O’Toole. Building on previous briefings, the TRM briefings flowed from the broader discussion about threats to MPs following the implementation of the Ministerial Direction.<sup>62</sup>

v. Briefings to Political Parties and Caucuses

37. Canada delivered unclassified briefings on FI to party caucuses in the House of Commons in June 2024.<sup>63</sup> These briefings were intended to raise levels of awareness of FI amongst MPs, and to provide specific information about protecting their “digital selves”.<sup>64</sup> These briefings were developed at the request of, and with input from, the Sergeant-at-Arms,<sup>65</sup> given his responsibility for the security of aspects of Parliament and MPs.<sup>66</sup> While there are allegations before this Commission that these briefings took too long to implement, these allegations ignore the context of both the extraordinary challenges of the COVID pandemic and, later, the 2021 election. In any event, MPs had already been alerted to the threat of FI by Minister Blair’s

---

<sup>59</sup> CSIS Threat Reduction Measures, [CAN.SUM.000028](#).

<sup>60</sup> CSIS Threat Reduction Measures, [CAN.SUM.000028](#), pp 2-3; Canadian Security Intelligence Service Stage 2 Institutional Report, Appendix G Overview of Foreign Interference Threat Reduction Measures 2019 – Present, [CAN.DOC.000017.003](#).

<sup>61</sup> Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), pp 67.

<sup>62</sup> Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), pp 56-60.

<sup>63</sup> Public Safety Canada, Public Hearing Transcript, [Volume 30](#), pp 132-133.

<sup>64</sup> Public Safety Canada, Public Hearing Transcript, [Volume 30](#), p 133.

<sup>65</sup> Minister LeBlanc, Public Hearing Transcript, [Volume 34](#), p 151; *In Camera* Examination Summary: Shawn Tupper, Tricia Geddes, Sebastien Aubertin-Giguere, [WIT0000144](#), para 53; Minister LeBlanc, Public Hearing Transcript, [Volume 34](#), p 151.

<sup>66</sup> Minister LeBlanc, Public Hearing Transcript, [Volume 34](#), pp 150-152.

December 2020 letter and the general threat briefings that are provided to all new MPs. As mentioned above, CSIS provided numerous defensive briefings to individual MPs.<sup>67</sup>

38. The SITE TF has also provided unclassified briefings to political party representatives in advance of each by-election since June 2023.<sup>68</sup> All political parties were invited.<sup>69</sup>

vi. Briefings to Political Party Leaders

39. Since 2023, Canada has offered classified briefings for political party leaders. These briefings are supported by tailored intelligence packages assembled to include the information that the party leader “needs to know”. The leader meets with security and intelligence officials and can ask questions to ensure that their own understanding is clear.<sup>70</sup> In order to receive Top Secret briefings, party leaders must obtain the required security clearance. Notably, being a member of the King’s Privy Council does not, in itself, entitle MPs or Leaders to access classified information.<sup>71</sup>

40. To date, the primary purpose of these briefings has been to inform party leaders of FI activities that may impact their members and their party so that they are equipped to take whatever steps they feel are necessary to protect their party against FI. These briefings allow them to use the tools that they have to address FI activities within their own parties, such as the ultimate approval of party candidates or appointment to various roles that might exacerbate particular risks.<sup>72</sup> Going forward, these briefings will cover topics beyond FI.

---

<sup>67</sup> Prime Minister’s Office, Public Hearing Transcript, [Volume 34](#), pp [31-32](#).

<sup>68</sup> Interview Summary: Security and Intelligence Threats to Elections Task Force (CSE Representative, Three CSIS SITE Representatives, Robin Wettlaufer, Greg O’Hayon, [WIT0000109](#), para [49](#); SITE TF Briefing to Unclassified Political Parties, [CAN044590](#); Security and Intelligence Threats to the Elections Task Force (SITE TF) Foreign Interference: A Threat to Canada’s National Security, [CAN044568](#); The Security and Intelligence Threats to Elections Taskforce, Public Hearing Transcript, [Volume 27](#), pp [153-154](#).

<sup>69</sup> Privy Council Office, Public Hearing Transcript, [Volume 29](#), pp [50, 80-83](#).

<sup>70</sup> *In Camera* Examination Summary: Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald, [WIT0000143](#), pp [8-9](#).

<sup>71</sup> As set out in the evidence, Ministers undergo a security assessment that, while different from a security clearance, is an equivalent process.

<sup>72</sup> *In Camera* Examination Summary: Prime Minister’s Office Senior Officials, [WIT0000163](#), para [27](#); Prime Minister Justin Trudeau, Public Hearing Transcript, [Volume 35](#), pp [59-67](#); Ad-Hoc Classified Briefings, [CAN047007](#).

vii. Cyber Support for Political Parties

41. The Canadian Centre for Cyber Security at CSE maintains a dedicated point of contact that political parties can reach out to on cyber security matters and provides advice and guidance to candidates on its website.<sup>73</sup>

*b) Canada has Partnered with Other Levels of Government*

42. FI affects not only all aspects of society, but all levels of government.<sup>74</sup> Cooperation between different levels of government is essential given Canada's constitutional division of powers.<sup>75</sup> While Canada's national security agencies can share information about FI and its possible impacts at the local and regional level, provinces and territories have jurisdiction over municipalities, education, digital media literacy and civics. They have a vital role in ensuring that democratic practices are passed on to successive generations.<sup>76</sup>

43. Canada has prioritized extensive engagement with provincial, territorial, municipal and Indigenous governments on FI and related issues. Canada has raised the need to increase digital and media literacy to defend against information manipulation, and the role that the provincial education system plays in increasing that literacy,<sup>77</sup> and has shared a Disinformation Guidebook and FI Toolkits.<sup>78</sup> Canada is also considering a national action plan on information manipulation that is integrated with provinces and territories.<sup>79</sup>

44. Canada's Ministers of Justice and Public Safety use their regular meetings with their counterparts to discuss issues of FI.<sup>80</sup> Senior officials, such as the Clerk of the Privy Council, the Commissioner of the RCMP and various Deputy Ministers, have discussed FI and related issues

---

<sup>73</sup> Communications Security Establishment Stage 1 Institutional Report, [CAN.DOC.000005](#), p 10.

<sup>74</sup> Country Summaries, [CAN.SUM.000030](#), p 4; Foreign Interference and You, [COM0000061](#), p 3; The Security and Intelligence Threats to Elections Taskforce, Public Hearing Transcript, [Volume 27](#), p 111; Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), pp 11-12.

<sup>75</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 77, 78-79.

<sup>76</sup> Privy Council Office, Public Hearing Transcript, [Volume 23](#), pp 189-190.

<sup>77</sup> *In Camera* Examination Summary: John Hannaford and Nathalie G. Drouin, [WIT0000150](#), para 41; Interview Summary: Department of Justice (Shalene Curtis-Micallef, Samantha Maislin Dickson, Heather Watts, Michael Sousa, [WIT0000100](#), para 18.

<sup>78</sup> Privy Council Office, Public Hearing Transcript, [Volume 23](#), pp 135-136; *In camera* Examination Summary: Allen Sutherland, Assistant Secretary to the Cabinet, Democratic Institutions and Machinery of Government, [WIT0000123](#), para 22.

<sup>79</sup> Interview Summary: Isabelle Mondou, Amy Awad, [WIT0000098](#), paras 32, 55.

<sup>80</sup> Minister LeBlanc, Public Hearing Transcript, [Volume 34](#), p 127.



with provincial, territorial and Indigenous counterparts, including the need to develop the security infrastructure to permit the sharing of classified information.<sup>81</sup> Similar discussions have occurred at the working level.<sup>82</sup> Finally, Canada helps to protect provincial, territorial and municipal electoral infrastructure, including by providing cyber resiliency advice and guidance.<sup>83</sup>

*c) Canada Coordinates with International Partners*

45. Canada hardly stands alone in its FI experiences; many of Canada's allies have experienced variations of these malign efforts. Canada engages on operational and policy discussions with its allies and peer nations to foster a collective response to the shared threat of FI in electoral processes and democratic institutions, and to draw from one another's national experience.

46. Among these, Canada's engagement with its Five Eyes allies is an invaluable international touchpoint and of critical value to Canada. The *raison d'être* of the Five Eyes alliance is intelligence-sharing.<sup>84</sup> Canada's understanding of FI is sophisticated, in part, because of the breadth of intelligence it shares and receives from its Five Eye partners.<sup>85</sup> These partners cooperatively share both operational information and policy development, including through the Intelligence Policy Forum (which coordinates the security and intelligence community within the Five Eyes on forward-looking policy in a rapidly-evolving space).<sup>86</sup> The Five Eyes also

---

<sup>81</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 77-78; Interview Summary: Department of Justice (Shalene Curtis-Micallef, Samantha Maislin Dickson, Heather Watts, Michael Sousa, [WIT0000100](#), para 18; Public Safety, Public Hearing Transcript, [Volume 30](#), p 138; Royal Canadian Mounted Police, Public Hearing Transcript, [Volume 27](#), at pp 9-10, 15-17, 24; *In Camera* Examination Summary: RCMP Commissioner Michael Duheme, Deputy Commissioner, Federal Policing, Mark Flynn, Assistant Commissioner, Federal Policing National Security, Brigitte Gauvin, [WIT0000137](#), para 31.

<sup>82</sup> Department of Justice (Shalene Curtis-Micallef, Samantha Maislin Dickson, Heather Watts, Michael Sousa, [WIT0000100](#), para 17.

<sup>83</sup> Interview Summary: Caroline Xavier, Rajiv Gupta, Alia Tayyeb, [WIT0000122](#), para 8-9.

<sup>84</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), p 19; Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), paras 43-44; Interview Summary: Royal Canadian Mounted Police (Commissioner Michael Duheme and Deputy Commissioner, Federal Policing, Mark Flynn), [WIT0000108](#), para 33; *In Camera* Examination Summary re: NSICOP Report: David Vigneault, Michelle Tessier, Cherie Henderson, Vanessa Lloyd, Bo Basler, [WIT0000136](#), para 26.

<sup>85</sup> Interview Summary: Caroline Xavier, Rajiv Gupta, Alia Tayyeb, [WIT0000122](#), para 53.

<sup>86</sup> Interview Summary: Privy Council Office – Security and Intelligence Secretariat, Intelligence Assessment Secretariat (Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald, Martin Green, Lisa Ducharme), [WIT0000110](#), para 5.

collaborate at the Ministerial level. In each of its alliances, Canada is increasingly recognized as a leader in countering FI.<sup>87</sup>

47. Canada has engaged internationally on best practices for detecting, deterring, and countering FI in elections collaboratively but with clarity. Officials have heard from the United Kingdom and France about their experience of FI in their elections<sup>88</sup> and from Taiwanese civil society groups at the forefront of detecting disinformation online.<sup>89</sup> Canada is learning from and working with international partners on the matter of regulatory frameworks for social media platforms, important to the success of democracies in thwarting disinformation.<sup>90</sup> In 2023, Canada, in partnership with the Netherlands, launched the first Global Declaration on Information Integrity Online which establishes a set of high-level international commitments to serve as a framework and guide for governments to uphold information integrity online.<sup>91</sup>

### **3. Canada is Building Public Resiliency to FI**

48. A well-informed citizenry, committed to democracy, is Canada's core defence against FI.<sup>92</sup> By shining a light on the threat, educating the population and fostering informed participation, a whole-of-society approach can actually take form.<sup>93</sup> Canada's public resilience will continue to grow through ongoing and future work among the public, cultural communities, and civil society organizations.

49. Like other democracies, Canada's response to information manipulation and disinformation is complicated by the technological difficulty of ascertaining the true actors behind information online, the need to balance taking decisive action on online FI with the right to freedom of expression, and the limited control any one country has over the content of the

---

<sup>87</sup> Interview Summary: Marco Mendicino, Member of Parliament for Eglinton—Lawrence, [WIT0000105](#), para [15](#); Interview Summary: The Honourable Dominic LeBlanc, [WIT0000103](#), para [24](#).

<sup>88</sup> Privy Council Office, Public Hearing Transcript, [Volume 23](#), p [148](#).

<sup>89</sup> Privy Council Office, Public Hearing Transcript, [Volume 23](#), p [164](#).

<sup>90</sup> Interview Summary: The Honourable Pascale St-Onge [WIT0000097](#), para [16](#); Minister St-Onge, Public Hearing Transcript, [Volume 33](#), pp [119-120](#).

<sup>91</sup> Interview Summary: The Honourable Mélanie Joly, [WIT0000096](#), para [13](#); Interview Summary: The Honourable Mélanie Joly, [WIT0000148](#), para [10](#); Minister Joly, Public Hearing Transcript, [Volume 32](#), p [128](#).

<sup>92</sup> Minister Gould, Public Hearing Transcript, [Volume 14](#), p [15](#).

<sup>93</sup> Public Safety, Public Hearing Transcript, [Volume 30](#), p [145](#); Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), pp [216-217](#); Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 4](#), pp [79](#).

internet. Canada continues to explore additional means to develop public resiliency to online information manipulation and disinformation.

50. Canada has greatly increased communications with the public, to ensure greater transparency about the nature of the FI threat, the government's response, and steps that can be taken by the public to protect themselves.<sup>94</sup> Canada has been making products relevant to FI in democratic processes and institutions publicly available in several languages since 2017 to foster awareness among cultural, religious and ethnic groups about FI threat actors and their methods.<sup>95</sup> Providing information to the public can also mitigate against a threat to public safety, as was recently done by the RCMP in the context of the involvement of agents of the Government of India in serious criminal activity in Canada.<sup>96</sup>

51. Importantly, this Commission has brought significant public attention to the threat of FI in electoral processes and democratic institutions. To assist in that effort, Canada has provided unprecedented access to classified information and Cabinet confidences in support of the Commission's work and has worked with the Commission to make as much of that information accessible to the public as possible.

*a) Collaboration with Cultural Communities*

52. Building trusted relationships with Canadian cultural communities is vital to Canada's efforts to detect, deter and counter FI as they are often the first victims. Both CSIS and the RCMP are dedicated to the development of such relationships, under the coordination of Public

---

<sup>94</sup> Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 15](#), pp [12](#); Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 10](#), pp [148-149](#); Canadian Security Intelligence Service Stage 2 Institutional Report, [CAN.DOC.000044](#), pp [16](#); Interview Summary: Caroline Xavier, Rajiv Gupta, Alia Tayyeb [WIT0000122](#), paras [4-5](#), [12](#), [51-52](#); *In Camera* Examination Summary: Caroline Xavier, Alia Tayyeb, Sami Khoury [WIT0000133](#), paras [5-15](#), [72-75](#); Communications Security Establishment, Public Hearing Transcript, [Volume 23](#), pp [10-19](#); Royal Canadian Mounted Police, Public Hearing Transcript, [Volume 27](#), p [21](#).

<sup>95</sup> Canadian Security Intelligence Service Stage 2 Institutional Report, [CAN.DOC.000044](#), pp [16](#); Royal Canadian Mounted Police, Public Hearing Transcript, [Volume 27](#), p [21](#); Privy Council Office, Public Hearing Transcript, [Volume 21](#), pp [140-142](#); Interview Summary: Caroline Xavier, Rajiv Gupta, Alia Tayyeb [WIT0000122](#), paras [4-5](#), [12](#), [51-52](#); *In Camera* Examination Summary: Caroline Xavier, Alia Tayyeb, Sami Khoury, [WIT0000133](#), paras [5-15](#), [72-75](#); Communications Security Establishment, Public Hearing Transcript, [Volume 23](#), pp [10-19](#) and [88](#); *In Camera* Examination Summary: Allen Sutherland, Assistant Secretary to the Cabinet, Democratic Institutions and Machinery of Government [WIT0000123](#), para [23](#).

<sup>96</sup> [RCMP statement on violent criminal activity occurring in Canada with connections to agents of the Government of India, October 14, 2024.](#)

Safety; however, Canada recognizes that more remains to be done.<sup>97</sup> Regular and formal opportunities for dialogue between the public and the government are essential to building these important relationships. To that end, the Cross-Cultural Roundtable on Security (Roundtable) provides advice and feedback to the Ministers of Public Safety and Justice.<sup>98</sup> Consultations with the Roundtable and other cultural community groups contributed to the robust framework to address nefarious activities that interfere with Canada's interests now found in the *Countering Foreign Interference Act*,<sup>99</sup> without marginalizing cultural communities or limiting their voice and political expression.<sup>100</sup> Continued interactions with communities allow the sharing of a wide range of perspectives, which in turn helps inform policy and advice to the government prepared by departments such as Public Safety.<sup>101</sup>

*b) Working with civil society organizations to build resilience*

53. A whole-of-society approach is required to address effectively the threat of FI through information manipulation and disinformation. Building a resilient and vigilant citizenry by bolstering the ability of Canadians to critically consider the media they consume, and partnering with civil society organizations such as CIVIX and Digital Public Square to actively call out disinformation, is critical to developing an effective response to FI.<sup>102</sup> Canada has a multi-pronged strategy that includes the Digital Citizen Initiative, the Canadian Digital Media Research Network, support for strong and independent media, and the Canadian Declaration on Electoral Integrity Online.

---

<sup>97</sup> *In Camera* Examination Summary: RCMP Commissioner Michael Duheme, Deputy Commissioner, Federal Policing, Mark Flynn & Assistant Commissioner, Federal Policing National Security, Brigitte Gauvin [WIT0000137](#), para 58; Public Safety Canada, Public Hearing Transcript, [Volume 30](#), pp 136-137; *In Camera* Examination Summary: Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère [WIT0000144](#), para 70; Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), p 89.

<sup>98</sup> Department of Justice Canada, Public Hearing Transcript, [Volume 23](#), pp 215-216.

<sup>99</sup> [Countering Foreign Interference Act, SC 2024, c 16](#).

<sup>100</sup> Department of Justice Canada, Public Hearing Transcript, [Volume 23](#), pp 215-219.

<sup>101</sup> *In Camera* Examination Summary: Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère [WIT0000144](#), para 78.

<sup>102</sup> Interview Summary: The Honourable Pascale St-Onge [WIT0000097](#), para 12.

i. Digital Citizen Initiative

54. The Digital Citizen Initiative aims to equip citizens with the tools that they need to make informed decisions as consumers of information, by building citizen resilience against online disinformation and building partnerships to support a healthy information ecosystem.<sup>103</sup>

55. Canada has also created the Digital Citizen Contribution Program, which supports the priorities of the Digital Citizen Initiative by providing time-limited financial assistance for research and citizen-focused activities. A recent focus was countering disinformation from foreign states, such as the PRC, and its impact on cultural communities.<sup>104</sup>

ii. Canadian Digital Media Research Network (CDMRN)

56. There are and should be limits on the state's ability to intervene in disinformation. In developing policies to address disinformation, Canada must balance freedom of expression with the potential harms caused.<sup>105</sup> Canadians have a right both to express themselves freely and to receive information online. It would be inconsistent with Canadian law and values for Canada to present itself as the ultimate arbiter of who is telling the "truth" in the online space.<sup>106</sup>

Government officials must exercise caution in commenting on false narratives online, particularly during an election, as they could risk overstepping their non-partisan role.<sup>107</sup>

57. Funded by Canada through a research grant,<sup>108</sup> the CDMRN is a network of researchers and academics, whose core consists of the Media Ecosystem Observatory (MEO).<sup>109</sup> Independent from government, the CDMRN monitors the domestic online ecosystem to detect information manipulation and whether this manipulation is having an impact or is being artificially amplified in the media ecosystem.<sup>110</sup> When an information incident is detected, such as the artificial spread

---

<sup>103</sup> Interview Summary: The Honourable Pascale St-Onge, [WIT0000097](#), para [12](#).

<sup>104</sup> Interview Summary: The Honourable Pascale St-Onge, [WIT0000097](#), para [13-14](#).

<sup>105</sup> Interview Summary: Isabelle Mondou, Amy Awad [WIT0000098](#), para [11](#).

<sup>106</sup> Interview Summary: Isabelle Mondou, Amy Awad, [WIT0000098](#), para [37](#).

<sup>107</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), p [199](#). Of note, attention is being directed at artificial amplification of information related to electoral processes.

<sup>108</sup> The DCCP provided the CDMRN with \$5.5 million in funding over 3 years, Canadian Heritage Institutional Report, [CAN.DOC.000034](#), p. [4](#); Media Ecosystem Observatory, Public Hearing Transcript, [Volume 22](#), p [60](#).

<sup>109</sup> Interview Summary: Media Ecosystem Observatory (Aengus Bridgman, Peter Loewen and Taylor Owen), [WIT0000089](#), paras [30](#), [40-41](#).

<sup>110</sup> Interview Summary: Media Ecosystem Observatory (Aengus Bridgman, Peter Loewen and Taylor Owen), [WIT0000089](#), paras [56-60](#); Media Ecosystem Observatory, Public Hearing Transcript, [Volume 22](#), pp [72-73](#).

of disinformation, the CDMRN responds with public alerts, incident updates, and incident summaries.<sup>111</sup> The CDMRN intends to monitor the domestic online ecosystem for information manipulation and its impacts during the next general election.<sup>112</sup> Although independent from government, the CDMRN's work informs government officials, including the Panel.<sup>113</sup> Its reports also inform Canada's policy work.<sup>114</sup>

iii. Supporting strong and independent media

58. Access to reliable, broadly accepted sources of information is a vital element in the democratic ecosystem. As a profession governed by well-understood ethical norms, traditional journalism institutions and practices play an important role in delivering fact-based information to the public. This fact-based information plays a key role in combatting misinformation and disinformation.<sup>115</sup>

59. Canada has adopted measures to support a strong and independent media ecosystem. The Local Journalism Initiative, the Canadian Journalism Labour Tax Credit, and the *Online News Act*<sup>116</sup> each respond to challenges presently faced by news organizations in receiving remuneration for their work. Canada has made a sound investment in its national public broadcaster to ensure citizens have access to reputable news sources.<sup>117</sup>

iv. Canada Declaration on Electoral Integrity Online (Declaration)

60. Canada collaborates with social media platforms to support fair, free and secure elections. The Declaration is a voluntary agreement between Canada and social media platforms which commits the platforms to a baseline of responsibilities around integrity and transparency.<sup>118</sup> It creates a contact point with the platforms and creates accountability for the platforms'

---

<sup>111</sup> Interview Summary: Media Ecosystem Observatory (Aengus Bridgman, Peter Loewen and Taylor Owen), [WIT0000089](#), paras 61-67.

<sup>112</sup> Interview Summary: Media Ecosystem Observatory (Aengus Bridgman, Peter Loewen and Taylor Owen), [WIT0000089](#), para 44.

<sup>113</sup> Interview Summary: Media Ecosystem Observatory (Aengus Bridgman, Peter Loewen and Taylor Owen), [WIT0000089](#), paras 32-33; Media Ecosystem Observatory, Public Hearing Transcript, [Volume 22](#), p 139.

<sup>114</sup> Interview Summary: Isabelle Mondou, Amy Awad, [WIT0000098](#), para 49.

<sup>115</sup> Interview Summary: The Honourable Pascale St-Onge, [WIT0000097](#), paras 3 & 5.

<sup>116</sup> [Online News Act \(S.C. 2023, c. 23\)](#).

<sup>117</sup> Interview Summary: The Honourable Pascale St-Onge, [WIT0000097](#), paras 6-9.

<sup>118</sup> *In Camera* Examination Summary: Allen Sutherland, Assistant Secretary to the Cabinet, Democratic Institutions and Machinery of Government, [WIT0000123](#), para 35.

commitment to reflect their community guidelines.<sup>119</sup> Four social media platforms signed the Declaration in 2019 and an additional three joined in 2021.<sup>120</sup>

61. Canada has been actively reengaging with various platforms on the Declaration in advance of the next general election. As one initiative, Canada has reached out to Tencent, the parent company of WeChat, about having the platform commit to the Declaration.<sup>121</sup>

#### **4. Canada's National Security Community has the Capacity to Detect, Deter and Counter FI**

62. Canada's national security community is guided by the Intelligence Priorities, which identify areas of strategic interest to the government every two years where intelligence support will be needed to advance Canadian interests. Based on these priorities, departments and agencies develop detailed Intelligence Requirements to guide their work.<sup>122</sup> For the period 2017-2019 to 2023-2025, Cabinet consistently identified FI in electoral processes and democratic institutions in Canada's Intelligence Priorities.<sup>123</sup>

63. Canada's national security systems for detecting, deterring, and countering FI in our electoral processes and democratic institutions are robust. Four agencies at the centre of Canada's FI response provide subject matter expertise in the areas of human source intelligence (CSIS), foreign signals intelligence and cybersecurity (CSE), foreign policy and online information manipulation (GAC) and law enforcement (RCMP). From investigating and laying criminal charges to coordinating diplomatic responses with like-minded states and allies to using TRMs to reduce and mitigate harm, Canada's national security community is equipped to detect, deter and counter all manner of FI activities. Operating under their respective mandates, these agencies protect Canada, our democratic institutions and processes, and our citizenry.

---

<sup>119</sup> *In Camera* Examination Summary: Allen Sutherland, Assistant Secretary to the Cabinet, Democratic Institutions and Machinery of Government, [WIT0000123](#), para 35.

<sup>120</sup> *In Camera* Examination Summary: Allen Sutherland, Assistant Secretary to the Cabinet, Democratic Institutions and Machinery of Government, [WIT0000123](#), para 36.

<sup>121</sup> Privy Council Office, Public Hearing Transcript, [Volume 23](#), p 138.

<sup>122</sup> *In Camera* Examination Summary: Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald, [WIT0000143](#), pp 6-7.

<sup>123</sup> Interview Summary: The Honourable Bill Blair, Minister of National Defence, [WIT00000102](#), para 8.

64. Through constant vigilance and the collaboration of government departments and agencies on the threat of FI, Canada’s democratic institutions and processes are strong and resilient. Canada, and Canadians, need to continue to build that strength.

65. The most recent legislative addition to Canada’s capacity to detect, deter and counter FI is C-70, the *Countering Foreign Interference Act*. Supported by all political parties in the House of Commons,<sup>124</sup> C-70 provides Canada’s national security agencies with modernized authorities to tackle the current and evolving tactics employed by hostile state actors. This Commission’s recommendations are welcomed for how to best counter future FI in light of the new tools available.

a) *CSIS - Intelligence Tools*

66. CSIS is well equipped to respond to FI with, amongst other things, warrants, defensive briefings, TRMs and the recent changes enacted by C-70. CSIS can now also issue unclassified security alerts to increase the awareness of the public or subnational governments of hostile state activities such as FI attempts.<sup>125</sup>

67. C-70 amended the *Canadian Security Intelligence Service Act*<sup>126</sup> to allow CSIS to better operate in a digital world and better respond to evolving threats.<sup>127</sup> It also authorized CSIS to share information with partners outside the federal government, subject to the appropriate security clearance and the “need to know”.<sup>128</sup> This change will help to build resiliency to FI throughout the Canadian population and enable FI-related investigations and prosecutions, such as through the sharing of information with premiers and provincial electoral bodies who have investigative authority.<sup>129</sup>

---

<sup>124</sup> Overview Report: Summary of *Countering Foreign Interference Act* (Bill C-70), [COM0000584](#), para 79; Interview Summary: The Honourable Dominic LeBlanc, [WIT0000103](#), para 21.

<sup>125</sup> *In Camera* Examination Summary: Canadian Security Intelligence Service Senior Officials, [WIT0000134](#), paras 25-28.

<sup>126</sup> *Canadian Security Intelligence Service Act*, [RSC, 1985](#), c C-23 (“*CSIS Act*”).

<sup>127</sup> Interview Summary: Canadian Security Intelligence Service, [WIT0000125](#), para 46.

<sup>128</sup> Interview Summary: Canadian Security Intelligence Service, [WIT0000125](#), para 46.

<sup>129</sup> Interview Summary: Canadian Security Intelligence Service, [WIT0000125](#), para 46.



*b) CSE – Foreign Signals and Cyber Defence Tools*

68. CSE, as Canada’s foreign signals intelligence collector, leverages all aspects of its mandate to detect, deter and counter FI activities,<sup>130</sup> including foreign cyber operations. As part of its cyber security and information assurance mandate, CSE provides advice, guidance and services to help protect electronic information and information infrastructure.<sup>131</sup>

69. CSE is an internationally recognized leader in cyber defence.<sup>132</sup> CSE uses a variety of sophisticated sensors to defend Canada’s systems, and other systems of importance, such as provincial and territorial elections infrastructure.<sup>133</sup> These sensors help detect suspicious activity and cyber incidents. CSE’s defences block an average of 6.6 billion attempted malicious actions a day against Government of Canada networks.<sup>134</sup>

70. When CSE learns of potential cyber threats, the Canadian Centre for Cyber Security coordinates with system owners to mitigate the threat. This is demonstrated by CSE’s response to the APT-31 tracking email link campaign targeting Parliamentarians’ email accounts. When CSE discovered malicious cyber activity originating from the PRC which targeted parliamentary systems, it immediately blocked the suspicious domain and informed House of Commons information security officials.<sup>135</sup> CSE provided classified briefings to House of Commons information security on the incident and provided numerous technical reports which included detailed recommendations.<sup>136</sup> With respect to any emails that were opened prior to mitigation measures being employed, the campaign would only have gathered high-level technical information about the receipt of the tracking email and did not collect any substantive

---

<sup>130</sup> Communications Security Establishment, Stage 2 Institutional Report, [CAN.DOC.000028](#), pp 3-4.

<sup>131</sup> PRC Email Operations Against Parliamentarians, [CAN.SUM.000027](#), para 2; Communications Security Establishment, Stage 2 Institutional Report, [CAN.DOC.000028](#), p 4.

<sup>132</sup> Communications Security Establishment Canada, Public Hearing Transcript, [Volume 23](#), p 34.

<sup>133</sup> Communications Security Establishment Canada, Public Hearing Transcript, [Volume 23](#), p 13.

<sup>134</sup> Communications Security Establishment Canada, Public Hearing Transcript, [Volume 23](#), p 34; Interview Summary: Caroline Xavier, Rajiv Gupta, Alia Tayyeb, [WIT0000122](#), paras 17, 20; PRC Email Operations Against Parliamentarians, [CAN.SUM.000027](#), para 5.

<sup>135</sup> *In Camera* Examination Summary: Caroline Xavier, Alia Tayyeb, Sami Khoury, [WIT0000133](#), para 31; Communications Security Establishment Canada, Public Hearing Transcript, [Volume 23](#), pp 36-49; see Chronology of Events [CAN.SUM.000027.001](#) for a chronology of actions taken by the Cyber Centre and CSIS to notify and aid House of Commons officials.

<sup>136</sup> Communications Security Establishment Canada, Public Hearing Transcript, [Volume 23](#), p 105-106.

information from the devices. This incident was successfully mitigated, and Parliamentarians' cyber security was not compromised.<sup>137</sup>

*c) GAC - Diplomatic Tools*

71. Diplomatic responses are important tools; they range from formal communications such as démarches and diplomatic notes, to public communications about Canada's position on issues, to denials of diplomatic visas, declaring diplomatic staff *persona non grata* (PNG) or closing foreign missions.<sup>138</sup> In concert with the actions of government agencies with a domestic mandate, GAC uses its diplomatic tools strategically to respond to FI. This includes bilateral engagements with countries engaging in FI to send a clear message that FI is unacceptable to Canada.<sup>139</sup>

*i. Bilateral Engagements*

72. When information supports the use of diplomatic tools, such as reliable information about inappropriate behaviour by diplomats, GAC and the Minister of Foreign Affairs act.<sup>140</sup> One example is the engagement with the PRC on the issue of FI, which ultimately resulted in the expulsion of Chinese diplomat Zhao Wei.<sup>141</sup>

73. Canada raised concerns about FI attempts with the PRC at various times and levels prior to 2023.<sup>142</sup> Additional irritants in the relationship included the so-called Overseas Police Stations, discussed elsewhere,<sup>143</sup> and Chinese spy balloons in Canadian sovereign airspace. Canada used frequent diplomatic communications to send the clear message that FI was unacceptable and there would be consequences if it continued.<sup>144</sup> These included a leader-to-leader warning that the Prime Minister conveyed to President Xi in November 2022, and denial of visas and positions to PRC diplomats.

---

<sup>137</sup> Communications Security Establishment Canada, Public Hearing Transcript, [Volume 23](#), pp 37-38.

<sup>138</sup> Global Affairs Canada Stage 2 Institutional Report, [CAN.DOC.000030](#), p 2.

<sup>139</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 27-32.

<sup>140</sup> Minister Joly, Public Hearing Transcript, [Volume 32](#), pp 115-117; Interview Summary: The Honourable Mélanie Joly, [WIT0000148](#), para 7.

<sup>141</sup> Declaration of Zhao Wei as PNG, [CAN.SUM.000016](#); Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 56-57.

<sup>142</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 51-58.

<sup>143</sup> People's Republic of China Police Stations, [CAN.SUM.000015](#).

<sup>144</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), p 31.

74. The potential expulsion of a PRC diplomat had been under active consideration throughout 2022 and 2023.<sup>145</sup> Media reporting naming Chinese diplomat Zhao Wei presented GAC with a further opportunity to send a firm message to the PRC and other countries contemplating or engaging in FI in Canada.<sup>146</sup> Seven days following the media report, the Minister of Foreign Affairs declared Zhao Wei PNG.<sup>147</sup> The PRC expelled a Canadian diplomat in response, as was expected.<sup>148</sup>

75. As it should, Canada uses diplomatic tools carefully, having regard to the bilateral and global contexts.<sup>149</sup> Countries that engage in FI do so as part of a broader strategy, and Canada must consider that bigger picture.<sup>150</sup> The foreign state may be seeking to provoke a reaction or to distract from other activities. The use of stronger tools, such as PNG, come with the expectation that the other country will respond with *at least* the expulsion of a Canadian diplomat. It may also respond more vigorously, such as when India expelled 41 Canadian diplomats following the Prime Minister's statement in the House of Commons regarding the murder of Hardeep Singh Nijjar.<sup>151</sup> The expulsion of Canadian diplomats harms Canada's interests. Without diplomatic presence, Canada loses advocates for its interests, the "eyes and ears on the ground" that it needs to be aware of the situation in the other country, and the channel it uses to communicate, including to address inappropriate behaviour.<sup>152</sup>

76. While the expulsion of diplomats must be done strategically, Canada will do so when the situation calls for it. Canada recently sent a very strong message to India that its FI and TNR activities were unacceptable with the expulsion of six Indian diplomats and consular officials.<sup>153</sup>

---

<sup>145</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), p 50.

<sup>146</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 49-52, 56.

<sup>147</sup> Minister Joly, Public Hearing Transcript, [Volume 32](#), pp 145-149.

<sup>148</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), p 57.

<sup>149</sup> Interview Summary: The Honourable Mélanie Joly, [WIT0000148](#), para 8.

<sup>150</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 11, 33.

<sup>151</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 59-62.

<sup>152</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), p 20.

<sup>153</sup> Prime Minister Justin Trudeau, Public Hearing Transcript, [Volume 35](#), pp 55-57.

ii. Multilateral Engagements

77. GAC's response to FI is not limited to acting against individual diplomats. Engaging with states implicated in FI activity can show that Canada is aware of it and does not tolerate it.<sup>154</sup> Further, engaging with the broader international community through multilateral organizations can bring greater awareness to FI and assist in developing international norms to counter it.<sup>155</sup> Canada is a leader in these efforts, confronting the threat of FI with our partners at the G7, G20, the North Atlantic Treaty Organization (NATO), the Association of Southeast Asian Nations (ASEAN) and on a bilateral level.<sup>156</sup>

iii. RRM Canada

78. Under Canada's leadership, the G7 nations developed the G7 RRM to share information on threats to democracy, with disinformation as a key focus.<sup>157</sup> The G7 RRM leverages Canada's international partnerships to permit a broader reach of awareness of threats to democracy. Canada is the permanent Chair of the G7 RRM, coordinating the broader G7 RRM network.<sup>158</sup> Within that network, RRM Canada monitors foreign open-source information such as social media for disinformation and information manipulation that would constitute threats to democracy.<sup>159</sup>

79. One example of the success of this initiative is the detection and countering of an incident of spamouflage in 2023. Based on information provided by a partner within the G7 RRM network, RRM Canada determined that the PRC was attempting to discredit a Canadian critical of the PRC by creating social media content, falsely attributed to that individual, which disparaged Canadian politicians. RRM Canada, with the approval of DMCIR, engaged with the

---

<sup>154</sup> See Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 67-68 for an example.

<sup>155</sup> See Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 47-48 for how this is being done in relation to the Declaration on Information and Integrity.

<sup>156</sup> Minister Joly, Public Hearing Transcript, [Volume 32](#), p 103; Interview Summary: The Honourable Pascale St-Onge, [WIT0000097](#), para 16.

<sup>157</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 34-35.

<sup>158</sup> Interview Summary: Global Affairs Canada (David Morrison, Alexandre Lévêque, Weldon Epp, Philippe Lafortune and Tara Denham, [WIT0000104](#), paras 6-7; *In Camera* Examination Summary: Global Affairs Canada (David Morrison, Cindy Termorshuizen, Alexandre Lévêque, Weldon Epp, Philippe Lafortune and Tara Denham, [WIT0000142](#), paras 29-32; Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 35-36.

<sup>159</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), p 37.

targeted Canadian and social media platforms, as well as politicians who had been disparaged in the false content.<sup>160</sup>

80. While RRM Canada has monitored the domestic information ecosystem during elections, and more recently by-elections, as part of the SITE TF, this work diverts the team from their mandate.<sup>161</sup> Canada recognizes the importance of monitoring the domestic online information ecosystem on an ongoing basis, not just during elections. Active discussions are underway to determine where this expertise should be located within the government structure.<sup>162</sup>

d) *RCMP - Law Enforcement Tools*

i. Disruption

81. The RCMP emphasizes its harm reduction and public safety mandate with the goals of disrupting FI-related activities and preventing them from recurring.<sup>163</sup> The act of disruption is exemplified by the RCMP's response to PRC Overseas Police Stations, described below.

ii. New criminal offences

82. Reflective of observed FI activities and after extensive consultations with a broad range of stakeholders,<sup>164</sup> new and updated offences created by C-70<sup>165</sup> authorize law enforcement to intervene in potential criminal FI activity sooner and in a broader range of circumstances.<sup>166</sup> Examples include the extraterritorial application of certain offences<sup>167</sup> and the creation of an offence for engaging in surreptitious or deceptive conduct with the intent to influence a political

---

<sup>160</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 81-83.

<sup>161</sup> Security and Intelligence Threats to Elections Task Force, Public Hearing Transcript, [Volume 27](#), pp 171-172; Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 38-41.

<sup>162</sup> Global Affairs Canada, Public Hearings Transcript, [Volume 28](#), pp 38-41; *In Camera* Examination Summary: Allen Sutherland, Assistant Secretary to the Cabinet, Democratic Institutions and Machinery of Government, [WIT0000123](#), para 55; *In Camera* Examination Summary: The Honourable Dominic LeBlanc, [WIT0000162](#), para 14; Minister LeBlanc, Public Hearing Transcript, [Volume 34](#), pp 134-135.

<sup>163</sup> *In Camera* Examination Summary: RCMP Commissioner Michael Duheme, Deputy Commissioner, Federal Policing, Mark Flynn and Assistant Commissioner, Federal Policing National Security, Brigitte Gauvin, [WIT0000137](#), paras 48-49.

<sup>164</sup> This included provincial, territorial and indigenous governments; stakeholders; industry; academics; and, affected communities.

<sup>165</sup> See for example section 20 of the *Foreign Interference and Security of Information Act*, RSC, 1985, c O-5 (“*FISOIA*”) and section 52 of the *Criminal Code*, RSC, 1985, c C-46.

<sup>166</sup> Royal Canadian Mounted Police, Public Hearing Transcript, [Volume 27](#), p 85.

<sup>167</sup> *FISOIA*, section 20.1; Interview Summary: Royal Canadian Mounted Police (Commissioner Michael Duheme and Deputy Commissioner Federal Policing, Mark Flynn), [WIT0000108](#), para 22.

or governmental process, which would apply to FI activity at different levels of government and school board elections as well as political party processes.<sup>168</sup>

*e) Public Safety - Regulatory Tools*

83. Canada is also establishing a Foreign Influence Registry (Registry), which will provide more transparency to Canadians about activities of influence conducted on behalf of foreign states. The Registry will require persons or entities who have a foreign influence arrangement to provide certain information to the Foreign Influence Transparency Commissioner. The Registry is meant to discourage foreign actors and states and their proxies from engaging in activities that interfere in Canadian affairs.<sup>169</sup>

## **5. The Government's Response to FI Threats is Coordinated**

84. Federal partners collaborate to ensure that the response to FI activities incorporates the mandates and perspectives of all agencies. This encourages the exchange of views to facilitate better decisions to counter the FI threat, aiming neither to underreact nor overreact.<sup>170</sup> This collaboration occurs at Cabinet committees, at the Deputy Minister level, through the National Counter Foreign Interference Coordinator and through effective intelligence dissemination.

*a) National Security Council (NSC)*

85. In 2023, the Prime Minister established a Cabinet committee for the consideration of national security issues, the NSC. The NSC was created to allow a strategic, whole of government approach to national security issues.<sup>171</sup> It allows for discussion with input from senior public service officials, where Ministers can deliberate on intelligence and provide

---

<sup>168</sup> *FISOLA*, section 20.4; Royal Canadian Mounted Police, Public Hearing Transcript, [Volume 27](#) p [85](#); Interview Summary: Royal Canadian Mounted Police (Commissioner Michael Duheme and Deputy Commissioner Federal Policing, Mark Flynn), [WIT0000108](#), para [22](#).

<sup>169</sup> *In Camera* Technical Briefing on Bill C-70, An Act Respecting Countering Foreign Interference: [Sebastian Aubertin-Giguère Associate Deputy Minister, National and Cyber Security Branch, Public Safety Canada, Nicole Giles Senior Assistant Deputy Minister and Deputy Director for Policy and Strategic Partnerships at CSIS, Greg Koster Director and General Counsel with the Criminal Law Policy Section at the Department of Justice, Mark Scrivens Senior Counsel at the Criminal Law Policy Section at the Department of Justice, and Sarah Estabrooks Director General of Policy and Foreign Relations at CSIS], [WIT0000132](#), paras [1](#) & [4](#).

<sup>170</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp [102-104](#).

<sup>171</sup> Interview Summary: The Right Honourable Justin Trudeau, [WIT0000106](#), para [16](#); Prime Minister Justin Trudeau, Public Hearing Transcript, [Volume 35](#), pp [25-26](#).

direction on policy orientation.<sup>172</sup> This complements the Incident Response Group, the Cabinet committee that would respond to specific incidents.<sup>173</sup>

86. The NSC drives Canada's response to strategic national security issues and is of significant value. It is a vital addition to the governance of the national security community, providing a dedicated Cabinet-level forum for the discussion of national security issues.<sup>174</sup> It provides an opportunity for a more deliberate use of intelligence in the context of policy and operational considerations, and results in a trickle-down effect as the discussions at NSC foster conversations that bring together the various implicated agencies.<sup>175</sup> The NSC has a fluid cycle, whereby the national security community can raise an issue, implement the NSC's direction, then return to the NSC with an assessment or new developments for further guidance.<sup>176</sup>

*b) Deputy Minister Coordination*

87. As part of the effort to increase and bolster coordination, Canada has revised the governance structure by which senior officials from across departments consider issues, including FI, from policy and operational perspectives. Key fora include: DMCIR, which discusses particularly sensitive and/or intelligence reporting that requires a timely response; the Deputy Minister Committee on National Security, which considers policy responses to national security issues; and, the Deputy Minister Operational Coordination Committee, which addresses operational actions related to intelligence and other information.<sup>177</sup>

---

<sup>172</sup> Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), para 12.

<sup>173</sup> *In Camera* Examination Summary: Deputy Clerk National Security and Intelligence Advisor and Deputy National Security and Intelligence Advisor, [WIT0000152](#), para 44.

<sup>174</sup> Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), para 12.

<sup>175</sup> Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), para 13; *In Camera* Examination Summary: John Hannaford and Nathalie G. Drouin, [WIT0000150](#), para 31.

<sup>176</sup> Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), para 13.

<sup>177</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 37-41; Privy Council Office Stage 2 Institutional Report, [CAN.DOC.000036](#), pp 26-27; Institutional Report for Privy Council Office, [CAN.DOC.000011](#), p 16.

88. The Elections Security Coordinating Committee, which includes Elections Canada senior officials as well as those of the core public service, ensures that Canada's core electoral infrastructure is protected against FI.<sup>178</sup>

*c) National Counter Foreign Interference Coordinator*

89. Detecting, deterring and countering FI, in democratic institutions and otherwise, involves many departments and agencies of the government and beyond. In recognition of the importance of this work, Canada appointed a National Counter Foreign Interference Coordinator (Coordinator), to coordinate Canada's policy approach to FI and to enhance transparency around the government's approach through public dialogue with all Canadians, including cultural groups, academia, non-governmental organizations and other domestic and international partners.<sup>179</sup> The Coordinator was heavily involved in the consultations regarding Bill C-70 and is now working to operationalize C-70.

*d) Intelligence Dissemination*

90. Canada has implemented processes to ensure intelligence is properly received and understood across government.<sup>180</sup> Whereas some intelligence products were previously shared by secure email, they are now housed on a secure database hosted by CSE, which allows for contemporaneous tracking of who has accessed specific products.<sup>181</sup> Properly cleared personnel in various departments and agencies are provided direct access to the database in order to review intelligence. In addition, individual public servants known as Client Relations Officers (CROs)

---

<sup>178</sup> Privy Council Office Stage 2 Institutional Report, [CAN.DOC.000036](#), pp [25](#) & [29](#); *In Camera* Examination Summary: Allen Sutherland, Assistant Secretary to the Cabinet, Democratic Institutions and Machinery of Government, [WIT0000123](#), para [16](#).

<sup>179</sup> Public Safety Stage 2 Institutional Report, [CAN.DOC.000040](#), p [1](#).

<sup>180</sup> Interview Summary: Caroline Xavier, Rajiv Gupta, Alia Tayyeb, [WIT0000122](#), paras [34-41](#); Canadian Security Intelligence Service Institutional Report, [CAN.DOC.000017](#), pp [6-7](#); Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), p [46](#); Global Affairs Canada, Public Hearing Transcript, [Volume 28](#), pp [54-55](#); *In Camera* Examination Summary: Deputy Clerk National Security and Intelligence Advisor and Deputy National Security and Intelligence Advisor, [WIT0000152](#), paras [7-10](#).

<sup>181</sup> Supplementary *In Camera* Examination Summary: Canadian Security Intelligence Service Senior Officials, [WIT0000135](#), para [52](#); Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), para [16](#).



remain tasked with disseminating intelligence through the targeted provision of intelligence products or verbal briefings, and with following up on any questions the recipients might have.<sup>182</sup>

91. As a specific example, Public Safety has seen a significant investment in the tracking of intelligence, with a dedicated group in charge of triaging and tracking intelligence sent to senior officials.<sup>183</sup> A CSIS liaison officer is posted at Public Safety to provide tailored packages of intelligence from Canadian collectors as well as allies.<sup>184</sup> This ensures the precise tracking of intelligence dissemination and the provision of more accurate and timely information to senior officials.<sup>185</sup> With the improved tracking of intelligence dissemination, Public Safety is able to identify more efficiently what is sent to its Minister.<sup>186</sup>

92. Additionally, there is a more rigorous and centralized process governing the intelligence sent to the Prime Minister's Office (PMO) and the Prime Minister to ensure the Prime Minister receives what he needs to see. This process is being refined and improved.<sup>187</sup>

93. While it is important to ensure the dissemination of information and intelligence is appropriately tracked, the receipt of individual pieces of intelligence must not be conflated with the situational awareness and understanding of the broader threat landscape necessary to take appropriate action. No senior decision maker should be expected to, nor should they, read every intelligence product produced by the national security community – approximately 71,000 in

---

<sup>182</sup> Supplementary *In Camera* Examination Summary: Canadian Security Intelligence Service Senior Officials, [WIT0000135](#), para 53; Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), para 17.

<sup>183</sup> Interview Summary: Public Safety Canada (Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère), [WIT0000095](#), para 6.

<sup>184</sup> Interview Summary: David Vigneault, Michelle Tessier, Cherie Henderson [WIT000041](#), p 7; *In Camera* Examination Summary: Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère, [WIT0000144](#), para 9; Public Safety Institutional Report (Part C), [CAN.DOC.000040](#), pp 19; Interview Summary: Public Safety Canada (Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère), [WIT0000095](#), paras 12-13.

<sup>185</sup> Public Safety Stage 2 Institutional Report, [CAN.DOC.000040](#), p 19.

<sup>186</sup> Interview Summary: Public Safety Canada (Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère), [WIT0000095](#), para 15.

<sup>187</sup> *In Camera* Examination Summary: Prime Minister's Office Senior Officials, [WIT0000163](#), paras 5-6; Interview Summary: The Right Honourable Justin Trudeau, [WIT0000106](#), para 2; Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), paras 14-18; Prime Minister's Office, Public Hearing Transcript, [Volume 34](#), pp 7-9; Prime Minister Justin Trudeau, Public Hearing Transcript, [Volume 35](#), pp 4-5.

2023 alone.<sup>188</sup> Triaging that “ocean of intelligence” into a manageable amount requires considerable judgement and understanding of the needs of the recipient.<sup>189</sup> It is understandable that more senior levels will see intelligence that is broader in scope, but fewer in terms of actual products.<sup>190</sup> For intelligence to be useful, it must add value to strategic or tactical policy considerations or be actionable.<sup>191</sup> In the case of the Prime Minister, he reasonably expects to see information that is directly impacting or threatening Canadians, that is linked to particular policy decisions that the government needs to make, or that he will need to know in advance of interactions with other leaders.<sup>192</sup>

94. Similarly, not all intelligence and related products are disseminated with the intention that the recipients will take action. Some are intended solely to inform,<sup>193</sup> as was the case with an Issues Management Brief advising senior officials about the defensive briefings of MPs.<sup>194</sup> While those listed as intended recipients could not recall seeing that particular product, they would not have done anything in response if they had.<sup>195</sup> In this situation, the fact that specific intended recipients did not recall seeing the product had no effect on Canada’s capacity to detect, deter or counter FI.

95. As many witnesses in the senior leadership of the government, elected or public officials, testified, they receive the information they need to take action to detect, deter and counter FI.<sup>196</sup>

---

<sup>188</sup> Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), para 18.

<sup>189</sup> *In Camera* Examination Summary: Deputy Clerk National Security and Intelligence Advisor and Deputy National Security and Intelligence Advisor, [WIT0000152](#), para 15 and 17.

<sup>190</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 30-31

<sup>191</sup> *In Camera* Examination Summary: John Hannaford and Nathalie G. Drouin ([WIT0000150](#), para 31)

<sup>192</sup> Prime Minister Justin Trudeau, Public Hearing Transcript, [Volume 35](#), pp 6-7.

<sup>193</sup> Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), pp 45.

<sup>194</sup> Defensive briefings to two Members of Parliament regarding PRC foreign interference activity, [CAN018796](#)

<sup>195</sup> Public Safety Canada, Public Hearing Transcript, [Volume 30](#), pp 14-19; Zita Astravas, Public Hearing Transcript, [Volume 31](#), pp 232-233; Minister Blair, Public Hearing Transcript, [Volume 33](#), p 13.

<sup>196</sup> Interview Summary: The Honourable Dominic LeBlanc, [WIT0000103](#), para 36; *In Camera* Examination Summary: Marco Mendicino, [WIT0000147](#), para 24; Minister Blair, Public Hearing Transcript, [Volume 33](#), p 43; Prime Minister Justin Trudeau, Public Hearing Transcript, [Volume 35](#).

## **D. Canada's Response to Specific Incidents and Allegations**

### **1. Political Party Processes are the Domain of Political Parties**

96. Political processes, including those undertaken by political parties, need to be safeguarded from FI. Political parties are private entities that have both the accountability and responsibility to make decisions about their party, including who may be allowed to represent the party at the local level.<sup>197</sup> This independence means that it is incumbent on political parties to ensure that their processes are robust.<sup>198</sup>

97. The government's role in helping political parties to address these potential vulnerabilities is not a binary question of whether or not to legislate; there are many options to help political parties strengthen their processes short of imposing legislation on them, such as increased transparency and briefings.<sup>199</sup> In addition, there are measures already in place to regulate areas of particular potential vulnerability, such as campaign donations.<sup>200</sup>

### **2. Public Service Debate about FI is a Strength, not a Weakness**

98. Different perspectives, and even debate, within the public service about whether certain activities constitute FI must not be mistaken as disagreements about the existence of FI or as a failure to respond. There is a working definition of FI that effectively guides the public service's approach to assessing situations on a case-by-case basis.<sup>201</sup>

99. Since the 2016 United States election, there has been a necessary and important evolution in perspective across the government on what constitutes FI and how the working definition might apply to a given set of circumstances. Hostile state actors are continuously changing their tactics. Discussion and debate are necessary.<sup>202</sup> Indeed, "groupthink" is dangerous in the national security space.<sup>203</sup> Given that FI actors intentionally operate in a manner to obfuscate their FI

---

<sup>197</sup> Elections Canada, Public Hearing Transcript, [Volume 21](#), pp 211-212

<sup>198</sup> Prime Minister Justin Trudeau, Public Hearing Transcript, [Volume 35](#), pp 75-76.

<sup>199</sup> Minister LeBlanc, Public Hearing Transcript, [Volume 34](#), p 157.

<sup>200</sup> Prime Minister Justin Trudeau, Public Hearing Transcript, [Volume 35](#), p 74.

<sup>201</sup> Global Affairs Canada, Public Hearing Transcript, [Volume 28](#), p 88; Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 124-125.

<sup>202</sup> Global Affairs Canada, Public Hearing Transcript, [Volume 28](#), pp 91-92, 94-95.

<sup>203</sup> Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), para 60.

activities, it is normal that different organizations approaching FI from different angles can arrive at disparate points of view and conceive of the same situation differently.<sup>204</sup> It is not just normal; it is intentional. Bringing different perspectives to bear when assessing information is a feature of the system and is encouraged.<sup>205</sup> This exchange of various perspectives and knowledge within the national security community when discussing FI results in better decisions on whether and how to respond.<sup>206</sup>

### 3. Overseas Police Stations

100. When a non-governmental organization publicly identified the existence of centres colloquially known as Overseas Police Stations providing services on behalf of the PRC government around the world, including in Canada, Canada acted quickly to investigate them and combat illegal activities. These stations offered services to the Chinese-Canadian community, but also appear to have collected intelligence and monitored former PRC residents living in Canada as part of the PRC's broader transnational anti-corruption, repression and repatriation campaign.<sup>207</sup>

101. In response, Canada took a series of diplomatic, mitigation and investigation activities.<sup>208</sup> GAC made clear to the Ambassador for the PRC that such stations were unacceptable under international law because they were providing government services at locations not accredited under the Vienna Conventions.<sup>209</sup> The RCMP acted immediately to disrupt these activities and investigated the stations to ensure that they closed.<sup>210</sup> This also demonstrated to the targeted communities that the RCMP was taking the issue seriously.<sup>211</sup> Canada's response to the Overseas Police Stations demonstrates both coordinated efforts within government, but also the need to

---

<sup>204</sup> Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), p [26](#).

<sup>205</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp [102-103](#).

<sup>206</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), p [103](#).

<sup>207</sup> People's Republic of China Police Stations, [CAN.SUM.000015](#).

<sup>208</sup> *In Camera* Examination Summary: RCMP Commissioner Michael Duheme, Deputy Commissioner, Federal Policing, Mark Flynn & Assistant Commissioner, Federal Policing National Security, Brigitte Gauvin, [WIT0000137](#), paras [50-52](#).

<sup>209</sup> Global Affairs Canada, Public Hearing Transcript, [Volume 28](#), pp [65-67](#).

<sup>210</sup> Royal Canadian Mounted Police, Public Hearing Transcript, [Volume 27](#), pp [26-30](#).

<sup>211</sup> *In Camera* Examination Summary: RCMP Commissioner Michael Duheme, Deputy Commissioner, Federal Policing, Mark Flynn & Assistant Commissioner, Federal Policing National Security, Brigitte Gauvin, [WIT0000137](#), para [50](#).

work closely with affected communities to ensure that they are safe and resilient to such activities.

#### **4. Targeting Paper and Special Report not being provided to the PM**

102. Not all intelligence products are intended for the Prime Minister.<sup>212</sup> As such, there should be no concern merely because certain intelligence products did not reach him. Some intelligence is for other audiences; other products are too preliminary in nature.<sup>213</sup>

103. The intelligence products that have come to be known as the “Targeting Paper” and the “Special Report” did not need to be seen by the Prime Minister. Neither would they have made any difference in his appreciation of the issues, for he was fully aware of the threat of PRC FI and the tactics used by hostile states, and fully engaged in formulating the response.<sup>214</sup> In neither case did the NSIA or senior PCO officials intend for these products to be seen by the Prime Minister.<sup>215</sup>

104. No detection, deterrence or countering activities went undone because the Prime Minister did not see these two intelligence products. Where there is intelligence that the Prime Minister needs to know, there are mechanisms in place to ensure that he is aware: the NSIA is the key official in that regard, but the NSC and Incident Response Group Cabinet Committees are also fora at which key intelligence on national security matters are discussed.<sup>216</sup> As well, the Clerk of the Privy Council has direct access to the Prime Minister and has often played a role in advising him on national security and intelligence issues.

#### **5. CSIS warrants and the timeline for one to be approved**

105. Allegations of political obstruction in the process for approving the application for “a warrant” were made in the hearing, without, it is respectfully submitted, any basis in fact. There

---

<sup>212</sup> Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), para 30.

<sup>213</sup> Interview Summary: Privy Council Office (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas & Stephen de Boer), [WIT0000116](#), para 29.

<sup>214</sup> Prime Minister Justin Trudeau, Public Hearing Transcript, [Volume 35](#), pp 13-16.

<sup>215</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 31 and 34.

<sup>216</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 42-47; Prime Minister Justin Trudeau, Public Hearing Transcript, [Volume 35](#), pp 26-32.

is no evidence of political interference or any other misfeasance by anyone involved in the approval of the application by the then Minister of Public Safety. There is also no evidence, or even specific suggestion, of any prejudice to the CSIS investigation by virtue of the passage of time.<sup>217</sup> The time taken to obtain Ministerial approval of every warrant application differs, depending on the nature of the warrant, the powers it seeks, whether it is a renewal, and whether there is any operational urgency related to the broader circumstances.<sup>218</sup>

106. Where a warrant application approval is urgent, there are processes to ensure that CSIS, Public Safety and the Minister's Office are all aware of the need to have it reviewed on an expedited basis. The direct relationship between the Director of CSIS and the Minister of Public Safety means that CSIS can bring a particular warrant directly to the Minister's attention if necessary.<sup>219</sup>

107. The Director of CSIS and the Deputy Minister of Public Safety did not identify any urgency to the warrant application at issue or have concerns about the timing of the Minister's approval.<sup>220</sup> The Minister's Chief of Staff denied delaying the warrant whether for partisan or any other reasons. She explained that there were numerous other issues demanding the Minister's attention at the relevant time, including lockdowns and vaccinations during the COVID pandemic. Other unclassified examples included updates to the list of terrorist entities, intelligence priorities, and policy discussions around 5G.<sup>221</sup> Senior CSIS officials also did not perceive that the Minister's Chief of Staff intentionally delayed the warrant.<sup>222</sup>

---

<sup>217</sup> Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), p [76](#); Zita Astravas, Public Hearing Transcript, [Volume 31](#), p [225](#); Minister Blair, Public Hearing Transcript, [Volume 33](#), pp [34-42](#); Public Safety Canada, Public Hearing Transcript, [Volume 30](#), pp [34-36](#).

<sup>218</sup> Public Safety Canada, Public Hearing Transcript, [Volume 30](#), pp [79-80](#), [193-194](#).

<sup>219</sup> Public Safety Canada, Public Hearing Transcript, [Volume 30](#), pp [34](#), [47](#) and [81](#); Addendum to *In Camera* Examination Summary: Mr. David Vigneault, Ms. Michelle Tessier and Ms. Cherie Henderson, [WIT0000121](#), para [9](#); *In Camera* Examination Summary: Rob Stewart, formerly Deputy Minister of Public Safety, Dominic Rochon, formerly Senior Assistant Deputy Minister, National and Cyber Security Branch, [WIT0000153](#), para [46](#).

<sup>220</sup> Addendum to *In Camera* Examination Summary: Mr. Rob Stewart, [WIT0000154](#), paras [6](#) and [8](#); *In Camera* Examination Summary: [Rob Stewart, formerly Deputy Minister of Public Safety, Dominic Rochon, formerly Senior Assistant Deputy Minister, National and Cyber Security Branch], [WIT0000153](#), paras [30](#) and [46](#); Public Safety, Public Hearing Transcript, [Volume 30](#), p [34](#); Addendum to *In Camera* Examination Summary: Mr. David Vigneault, Ms. Michelle Tessier and Ms. Cherie Henderson, [WIT0000121](#), para [9](#).

<sup>221</sup> Zita Astravas, Public Hearing Transcript, [Volume 31](#), pp [222-226](#), [252](#), [275](#) & [279](#).

<sup>222</sup> Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), p [76](#).

108. The warrant application in question was approved by the Minister immediately on his review, and the warrant was granted by the Federal Court.<sup>223</sup> The explanation provided, that the Chief of Staff did not prioritize a warrant that the Director of CSIS did not flag as urgent, is entirely reasonable and consistent with the evidence. Canada notes that the Commission was able to explore this matter, among others, in greater detail *in camera*. Each of the witnesses who testified in public about the warrant was unable to address certain facts or respond to certain allegations on the basis of national security confidentiality. Their inability to publicly address classified matters with full detail is not a fair or reasonable basis to impugn their conduct or speculate about misfeasance, in this or any other matter before the Commission.

## **6. Hostile Activities by State Actors (HASA) Memorandum to Cabinet and Bill C-70**

109. The evidence is clear that FI is complex, international in scope and that hostile state actors continuously change their tactics.<sup>224</sup> Canada is a nation that values the rule of law and the *Canadian Charter of Rights and Freedoms* while also responding to evolving threats. Some have suggested that more could have been done sooner, including advancing the HASA initiative and the introduction of Bill C-70. Canada does not agree. These very significant initiatives took care and time; some requiring extensive consultations. When it comes to building a societal response to a complex problem, and when the expressive rights and democratic rights of Canadians are on the line, care is not delay.

### **E. Canadians Can and Should have Confidence**

#### **1. Confidence in 43<sup>rd</sup> and 44<sup>th</sup> General Elections**

110. The Commission has had unprecedented access to classified information and intelligence. Based on that information, the Commission can and should conclude that Canada's federal elections and democratic processes are sound. The evidence demonstrates that FI did not affect

---

<sup>223</sup> *In Camera* Examination Summary: Zita Astravas, [WIT0000158](#) para 51; National Security and Intelligence Committee of Parliamentarians, Annual Report 2020, [COM0000156](#); Minister Blair, Public Hearing Transcript, [Volume 33](#), p 96.

<sup>224</sup> Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), p 239.

which party formed government in 2019 or 2021.<sup>225</sup> The general elections in 2019 and 2021 were free and fair; the outcome was decided by Canadians.

## 2. Confidence in Democratic Processes

111. While FI in Canada's electoral processes and democratic institutions is a significant threat, the government is alert and continues to develop its capacity to detect, deter and counter the threat.<sup>226</sup> It is important neither to understate nor overstate the seriousness of the threat.<sup>227</sup> Canada has not been the target of a nation-wide campaign intended to undermine our electoral processes or democratic institutions, as seen in other countries.<sup>228</sup>

### *a) Media reporting on FI in late 2022 and early 2023*

112. The media reporting on FI in late 2022 and early 2023, based on illegal leaks, unnecessarily and misleadingly shook the confidence of Canadians in the integrity of our electoral processes and democratic institutions. The unauthorized disclosure of classified information proved to be an obstacle in increased public understanding and meaningful discourse on FI. The leaks may even have helped foreign threat actors meet their FI objectives. It was illegal, irresponsible, and rashly jeopardized not only our national security agencies' sources and methods, but also the confidence Canadians have in their government's ability to respond to threats leveled against Canada. Indeed, the Independent Special Rapporteur on Foreign Interference, who reviewed the underlying classified information (which has been made available to the Commission), concluded that when the intelligence reported in the media was considered in context, the issues were less concerning or in some cases told a different story than what was reported.<sup>229</sup>

113. When selective or incomplete classified information enters the public domain without proper context, it may be interpreted incorrectly.<sup>230</sup> Intelligence agencies are unable to comment

---

<sup>225</sup> [Initial Report](#), pp142-143.

<sup>226</sup> [FISOLA](#); Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), pp 79 & 216.

<sup>227</sup> Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 189-190.

<sup>228</sup> Global Affairs Canada, Public Hearing Transcript, [Volume 28](#), pp 221-222; Suspected Instances of Foreign Interference, CAN.SUM.000031\*document unavailable on Commission website; Privy Council Office, Public Hearing Transcript, [Volume 31](#), pp 195-198.

<sup>229</sup> National Security Intelligence Officials, Public Hearing Transcript, [Volume 4](#), pp 81-82.

<sup>230</sup> National Security Intelligence Officials, Public Hearing Transcript, [Volume 4](#), p 85.



on leaked intelligence because doing so may reveal classified information.<sup>231</sup> As a result, incorrect and incomplete allegations circulate in public without the possibility of clarification or correction.<sup>232</sup> A responsible information environment is a bedrock of democracy, for this and many other reasons.

114. Building on the conclusion set out in its First Report, this Commission has the opportunity to clarify for the public a clearer understanding of the nature and extent of the threat and confirm that Canadians can and should have confidence in their democratic institutions.

### **3. Confidence in Parliamentarians**

115. The NSICOP Special Report on Foreign Interference in Canada’s Democratic Processes and Institutions (NSICOP Special Report), tabled in Parliament on June 3, 2024, has been interpreted by some to mean that Parliamentarians are working for other countries or that some are “traitors”. NSICOP is an important Parliamentary body which contributes to national security and increases transparency.<sup>233</sup> The Commission has had the opportunity to review the unredacted version of the NSICOP Special Report and examine both the underlying intelligence and witnesses and is therefore able to provide its independent view of the NSICOP assessments and place them in suitable context.

116. CSIS witnesses testified they had reservations regarding some of NSICOP’s factual findings. They view the NSICOP Special Report as generally accurate in outlining the nature of the threat but indicated that the assessments or wording were stronger than CSIS might have chosen. More specifically, CSIS witnesses testified that there were factual discrepancies between the CSIS intelligence and the findings in the NSICOP Special Report,<sup>234</sup> and that some of the intelligence relied on by NSICOP contained factual errors or was taken to be more definitive than it was.<sup>235</sup>

---

<sup>231</sup> National Security Intelligence Officials, Public Hearing Transcript, [Volume 4](#), pp [77-78](#).

<sup>232</sup> National Security Intelligence Officials, Public Hearing Transcript, [Volume 4](#), p [78](#).

<sup>233</sup> Prime Minister Justin Trudeau, Public Hearing Transcript, [Volume 35](#), p [78](#).

<sup>234</sup> Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), pp [117-118](#), [127-128](#).

<sup>235</sup> Canadian Security Intelligence Service, Public Hearing Transcript, [Volume 24](#), pp [119-121](#), [123-127](#).

117. The NSIA noted that the NSICOP Special Report had lost the nuances of the intelligence through its summarizing of intelligence, which is always a challenge.<sup>236</sup> She has not seen evidence of any MP who undertook espionage or sabotage activities or any MP that has imperiled the security of Canada.

**F. Conclusion**

118. While FI is both present and evolving, Canadian electoral processes and democratic institutions processes are sound. Canada's understanding of FI and its defences against FI are strong. Canada continues to refine those defences. The government recognizes the need for unwavering vigilance and steadfast resolve.

119. Canada welcomes the recommendations of the Commission to further bolster its defences, and thanks the Commission for its careful study of these important and challenging issues.



---

Gregory Tzemenakis  
Senior General Counsel  
**Counsel for the Government of Canada**



---

Barney Brucker  
A/Senior General Counsel  
**Counsel for the Government of Canada**

---

<sup>236</sup> *In Camera* Examination Summary: John Hannaford and Nathalie G. Drouin (House Motion), WIT0000149, para 23. \* document unavailable on Commission website