IN THE MATTER OF THE PUBLIC INQUIRY INTO FOREIGN INTERFERENCE IN FEDERAL ELECTORAL PROCESSES AND DEMOCRATIC INSTITUTIONS

AFFIDAVIT OF NEWTON SHORTLIFFE

I, Newton Shortliffe, of the City of Ottawa, in the Province of Ontario, AFFIRM THAT:

1. On June 19, 2024, I was interviewed by Counsel to the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions ("Commission Counsel") in my capacity as the Assistant Director, Collection of the Canadian Security Intelligence Service (CSIS) from May 2021 to July 2024. I was interviewed as part of a panel of current and former CSIS officials, alongside René Ouellette, Bo Basler, Dr. Nicole Giles, David Vigneault, Vanessa Lloyd, Cherie Henderson and Adam Fisher.

2. In advance of the Stage 2 public hearings, Commission Counsel prepared a public summary of our interview, which was reviewed for National Security Confidentiality ("NSC").

3. In the course of the NSC review, some of the information was removed or summarized in order to protect the disclosure of information that could be injurious to the critical interests of Canada or its allies, national defence or national security.

4. I have reviewed the public summary of our interview, a copy of which is attached as **Exhibit "A"** to this affidavit (the "Unclassified Interview Summary").

5. The Unclassified Interview Summary contains an accurate account of the publicly disclosable information that I provided to the Commission. I do not wish to make any changes, additions, or deletions to the Unclassified Interview Summary. Insofar as the Unclassified Interview Summary contains information provided by other interview participants, that information is accurate to the best of my knowledge and belief.

6. I adopt the contents of the Unclassified Interview Summary ascribed to me as part of my evidence before the Commission.

AFFIRMED before me in the City of Ottawa,
in the Province of Ontario on October 22, 2024.

Commissioner for Taking Affidavits

Newton Shortliffe

A COMMISSIONER ETC. JUSTIN ROY WHILE BEING A BARRISTER & SOLICITOR LSO #80222O PROVINCE OF ONTARIO

This is **Exhibit "A"** to the Affidavit
of Newton Shortliffe, affirmed before
me on October 22, 2024

Commissioner for Taking Affidavits

Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions | Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Interview Summary: Canadian Security Intelligence Service

Commission Counsel interviewed officials from the Canadian Security Intelligence Service ("**CSIS**" or "**the Service**") on June 19, 2024. The interview was held in a secure environment and included references to classified information. This is the public version of the classified interview summary that was entered into evidence in the course hearings held *in camera* in July and August 2024. It discloses the evidence that, in the opinion of the Commissioner, would not be injurious to the critical interests of Canada or its allies, national defence or national security.

Notes to Reader:

- Commission Counsel have provided explanatory notes in square brackets to assist the reader.

1. Interviewees

[1] René Ouellette is the Service's Director General ("**DG**") of Academic Outreach and Stakeholder Engagement. He has held that position since November 2019.

[2] Bo Basler is the Service's Counter-Foreign Interference Coordinator ("**CFIC**"), a role he assumed in March 2023. Prior to that, he served as a Regional Director General and Regional Deputy Director General.

[3] Dr. Nicole Giles is the Service's Senior Assistant Deputy Minister and Deputy Director for Policy and Strategic Partnerships. She has served in that role since October 2022. She previously served as Assistant Deputy Minister, at Immigration, Refugees and Citizenship Canada. She also served with Global Affairs Canada as an ambassador to Guyana and Suriname.

[4] David Vigneault has been the Service's Director since 2017.

[5] Vanessa Lloyd is the Service's Deputy Director of Operations ("**DDO**"). She was appointed in May 2023. From 2020 to her appointment as DDO, she held a senior executive position at CSIS focused on transformation and modernization.

[6] Cherie Henderson served as the Service's DG of the Intelligence Assessment Branch ("**IAB**") from 2019 to 2022. There, she oversaw the production and dissemination of intelligence reports. In 2021, she became Acting Assistant Director, Requirements, formally assuming the role in 2022 until her retirement in 2024.

[7] Newton Shortliffe was the Service's Assistant Director, Collection ("**ADC**") from May 2021 to July 2024. He oversaw all collection activities at CSIS. He has served in various positions at CSIS since 1990, including as a Regional Director General.

[8] Adam Fisher is the DG of the Service's Litigation and Disclosure Branch. He has held that position since the autumn of 2023. He oversees the *One Vision* framework [the *One Vision* framework governs the exchange of information between CSIS and the Royal Canadian Mounted Police ("**RCMP**")] as well as the disclosure of information held by CSIS during legal proceedings and in response to access to information and privacy requests. He served as DG IAB from 2016 to 2019, and from 2021 until his current appointment. Prior to that, he was the Director of Operations at the Security and Intelligence Secretariat of the Privy Council Office ("**PCO**").

2. Evolution of the Threat Landscape

2.1 Specific Threat Actors

[9] Ms. Henderson explained that CSIS has observed foreign interference ("**FI**") in electoral processes for over 25 years. She referred to a suspected incident of FI, which took place decades ago involving a proxy of the People's Republic of China ("**PRC**"). She noted that CSIS has continued to observe hostile foreign actors approach elected officials with increasing frequency.

[10] After the attacks of September 11, 2021, the Service's priorities and resource allocation shifted towards counter-terrorism. CSIS still monitored the FI threat. Ms. Henderson said the PRC's knowledge of Canadian laws and democratic institutions has enabled it

to play federal and provincial governments against each other and create divisions between levels of government. The PRC has also sought to cultivate relationships with Indigenous governments and groups.

[11] Ms. Henderson said that the PRC had increased its FI capabilities and that Canadians do not fully understand how hostile actors leverage Canada to their advantage.

[12] Ms. Henderson added that Russia has also been a constant threat, particularly in espionage.

[13] Ms. Henderson explained that India is mainly concerned with Canada's perceived lack of response to Khalistani terrorism, a prime concern to India. She noted that Canada's relationship with India tends to vary significantly depending on the broader geopolitical context.

[14] Ms. Henderson noted that other actors, such as Iran, do not focus their threat activities on democratic institutions. They focus instead on repressing members of their diaspora communities in Canada.

[15] Ms. Lloyd added that CSIS monitors the threat activities of these actors in a holistic fashion, not just for FI in democratic processes. Viewed through this broader lens, the intensity and risk of the threat they pose varies greatly over time. Mr. Vigneault explained that there is no clear distinction between FI targeting democratic processes and other forms of FI, such as transnational repression in the *CSIS Act*. He noted that, while the threat activities of some actors only seek to repress their diasporas, most foreign state actors target diasporas as well as other, different, aspects of the Canadian social fabric. He said that before the 2016 American election, FI in democratic institutions was not a significant strategic issue for hostile state actors, except China.

[16] Dr. Giles stated that the distinctive characteristic of the PRC's activities is the magnitude of its objectives and its patience for achieving them – to project a positive image of the CCP regime throughout the globe, to preserve the stability of the PRC, and to influence the global order and rules. Mr. Fisher agreed and emphasized that, along with this broad set of objectives, the PRC also seeks to repress its diaspora members, with a specific focus on the Five Poisons [entities associated with the Falun Gong,

Taiwan/Taiwanese independence, Tibet/Tibetan independence, Xinjiang separatism/Uyghur minorities, and pro-democracy movements (especially in relation to Hong Kong)].

2.2 Technologies and Tactics

[17] Commission Counsel referred the interviewees to a CSIS intelligence product that outlined security concerns over the use of a particular technology. Mr. Vigneault explained that, in the face of evolving technologies and threats, the principal mandate of CSIS remains to advise and inform the Government of Canada. Mr. Vigneault recalled that CSIS had issued a security alert recommending caution in the use of particular PRC-manufactured technology. He noted that, where a technology is already implemented and in use, there are challenges to implementing the Service's recommendations: removing and replacing the technology may be costly, and the provider of technology may sue the Government for reputational harm.

[18] Mr. Vigneault added that one objective of CSIS is to ensure that municipalities and provinces make informed decisions in using technology and that they are aware of the threats that they face. He noted, for example, the challenge for municipalities that may rely on new technologies to develop initiatives such as "smart cities" and improve infrastructure. While these technologies can be helpful, they can equally be vectors for FI. It is important for CSIS to work with municipalities to help them better understand the insidiousness of some technologies and the different, not immediately apparent, vectors for FI.

[19] Ms. Henderson agreed with Mr. Vigneault that the primary goal is to raise awareness about the dangers of technology, although this can be challenging when CSIS is limited in what intelligence it can share. This had led CSIS to develop security alerts at a lower classification, a product to inform civil society of a threat without necessarily disclosing classified information. Ms. Henderson noted that using security alerts could cause CSIS to run significant legal risks, such as risks of lawsuits. She also indicated that the effectiveness of these tools may be limited when an entity is already using the technology at issue. It can be hard to tell governments that the technologies they just

purchased were a waste of money. Ms. Lloyd agreed that CSIS could share information related to a threat with civil society either through a security alert or by implementing a threat reduction measure ("**TRM**").

[20] Dr. Giles explained that CSIS has attempted to increase transparency and build more robust frameworks to govern its sharing of information and provision of advice. Dissemination of intelligence is a shared responsibility within government but the goal is to ensure that information CSIS provides is received and acted on appropriately. She noted that national security concerns are not always on other government departments' radars, namely those entities whose mandates do not fall squarely under the national security umbrella or whose entities may not be traditional partners of the national security community. Being able to have a sophisticated national security dialogue with these entities to ensure that national security concerns can factor into their decision-making is important. Government procurement is one example. Mr. Ouellette gave the further example of research and academia and noted that it was challenging to educate these stakeholders. Ms. Henderson stated that the *Investment Canada Act* ("**ICA**") allows departments to assess one transaction at a time; however, CSIS has been able to use the *ICA* to demonstrate to Government patterns of behaviour contrary to Canada's national interest when it carries out assessments under that *Act*. CSIS' advice can be considered to block transactions that may pose threats to the security of Canada.

[21] Mr. Basler said technology acts as an amplifier of the intent of foreign states. Dr. Giles agreed and added that, with technology, apparently innocuous activity can have a dual purpose, for example Tik Tok – it is a platform to watch videos but there remains the concern that large quantities of data about its users is vulnerable to being accessed by the PRC.

[22] Mr. Vigneault was asked whether there is any international regulation of the sale or acquisition of spyware or surveillance technologies. He said that, while the United Nations is looking to adopt normative frameworks, the use of these technologies remain mostly unregulated, even more so outside the Five Eyes. Regulating cyber threat technology is challenging because the evolution of technology far outpaces government

regulation efforts. Furthermore, some foreign threat actors may hide behind the veil of their domestic laws to justify their use of cyber threat technology, but Canadian law limits Canadian security agencies, including the RCMP, in their use of these technologies.

[23] Dr. Giles stated that the PRC has almost unlimited resources to leverage technology for its threat activities. Mr. Shortliffe noted that the data that the PRC collects today can, in the future, be processed by more potent technology. Cyber threats are a long-term concern. Threat actors harvest information today for use tomorrow.

3. Public Reporting and Transparency

[24] The interviewees were referred to an excerpt of a CSIS Intelligence Assessment entitled "Canada Towards 2028",[1] which reads as follows:

> Similarly, a more mature, less hesitant, public- and private-sector outreach strategy on CI [counterintelligence] threats will be required to better sensitize potential targets on the CI threat, including insider threat activity and communities targeted for infiltration by foreign states. This strategy would include training SMEs [subject matter experts] and IOs [intelligence officers] for sector-specific outreach. We also need to bring our Public Report more in line with other allied services that have offered far more detailed and substantive discussions of threat issues. A "taking it to the people" strategy will, for example, help support threat reduction measures (TMRs) by encouraging a general public that is more aware and by instilling a normative national security culture in the population.

[25] Dr. Giles indicated that this passage reflects why CSIS has leaned heavily into increasing transparency over the past 18 months. CSIS had made great strides in this respect, including by releasing detailed statistics for the first time in the Service's 2022 Public Report about its threat surveillance and threat mitigation activities. The Service's 2023 Public Report has gone even further by including detailed threat assessments and spotlights on core aspects of the Service's mandate as well as on executive members working at the Service. She viewed these efforts as a necessary tool to counter the pernicious FI threat. Mr. Ouellette added that CSIS has increased its efforts to meet with

[1] CAN038232.

universities, industry and research institutions, Indigenous partners and other stakeholders to talk about the threats posed by the PRC. These engagements aim to build trust and inform stakeholders about how the threat is relevant to their work.

[26] Mr. Basler added that the Public Inquiry into Foreign Interference (the "**Commission**") and the Service's efforts to share information with the Commission, and to make public so many documents and topic summaries, were also an illustration of CSIS' commitment to transparency and educating the public about the FI threat.

[27] Mr. Vigneault added that CSIS does not intend to be sanctimonious in its outreach but instead attempts to inform Canadians. He gave an example illustrating a case where outreach to warn a company about FI threats had proven to be effective in preventing infiltration by foreign state actors. Ms. Lloyd, for her part, noted that the focus of the Service's engagement has shifted as its priorities have evolved from counter-terrorism to counter-intelligence.

4. Internal Coordination

[28] The interviewees were referred to an excerpt of an operational branch's Plan for 2023-2024. The excerpt indicates that a key output is to expand briefings to parliamentarians and an objective is to support the CSIS Foreign Interference Tiger Team ("**C-FITT**"). Ms. Lloyd said that this document reflects the branch's planned activities and intended outcomes.

[29] Mr. Shortliffe stated that this branch works with the regional offices to develop the priorities for intelligence collection based on available resources. As an example of resource allocation, CSIS continues to provide defensive briefings both proactively and when asked and the regional offices usually deliver them. Ms. Lloyd and Mr. Basler explained that organizing and delivering some defensive briefings was temporarily paused when C-FITT was stood up and started to organize and/or deliver the briefings. This allows the operational branch to better focus on its operational work.

[30] Mr. Basler explained that C-FITT reflects the Service's need to shift towards a more thematic approach to FI in the present environment. This contrasts with the former

structure where FI was addressed in silos by each branch. He noted that CSIS is currently coordinating with other departments to try to set a common definition of FI across the Government of Canada, as it had previously done with counter-terrorism and ideologically motivated violent extremism. Mr. Vigneault noted that this has been challenging and gave the example of Global Affairs Canada ("**GAC**"), whose conceptualization of FI is not necessarily the same as that of CSIS.

[31] Mr. Basler said C-FITT has three pillars of work:

a) Development of a broader FI strategic and policy framework internally and to lead from behind with the rest of Government. This includes Communication within CSIS and externally with the rest of government. He noted that this had led to the development of a single presentation to Members of Parliament that is now used across departments to brief about the FI threat;

b) Coordination of the Service's response to support the work of the Commission, NSIRA, NSICOP and the Independent Special Rapporteur; and

c) Taking on the role of Chair and integrating the Security and Intelligence Threats to Election Task Force ("**SITE TF**").

[32] Mr. Ouellette added that Bill C-70 also sought to enable information sharing with a broader public audience.

5. Specific Information Flow Incidents

5.1 The "Targeting Paper"

[33] Mr. Vigneault was asked about an intelligence product, which a National Security Review Agency ("**NSIRA**") review[2] (the "**NSIRA Report**") refers to as the "Targeting Paper". [Both the NSIRA report and the National Security and Intelligence Committee ("**NSICOP**") Special Report on Foreign Interference in Canada's Democratic Processes and Institutions (the "**NSICOP Report**") state that the CSIS Director believed that the

[2] Review of the dissemination of intelligence on People's Republic of China political foreign interference, 2018-2023 (the "NSIRA Report").

Targeting Paper should be provided to the Prime Minister. The Prime Minister did not receive it.]

[34] Mr. Vigneault explained that the Targeting Paper provided a comprehensive overview of the PRC's strategy to "target" federal Canadian political actors for influence operations [CSIS comment: targeting for the purposes of foreign interference operations]. A CSIS senior analyst drafted the Targeting Paper, which Mr. Vigneault described as one of the most informative reports on the capabilities and tactics of the PRC.

[35] Mr. Vigneault explained that the Targeting Paper had gone through more than one iteration. Due to a number of factors, the initial version of the document, which listed names of potential targets was shared with a small number of Deputy Ministers ("**DMs**"). The DMs who viewed the report were surprised by its contents, and discussed the need to be careful about not disseminating it too widely.

[36] Mr. Vigneault stated that he had first learned that the Targeting Paper had not been shared with the Prime Minister during NSIRA's review. He was not consulted about whether it should be shared with the Prime Minister and did not know why the Prime Minister did not receive it. When asked if CSIS would have liked the Targeting Paper to have been shared with the Prime Minister he responded in the affirmative. Mr. Basler added that his understanding was that the intent was to share the more sanitized version of the Targeting Paper titled, "PM Version" with the Prime Minister.

[37] Ms. Henderson added that, in addition to believing that the Targeting Paper should be presented to senior officials, CSIS also intended to use an unclassified version of it to educate MPs in an unclassified setting so as to make the document as useful as possible.

5.2. The "PCO Special Report"

[38] Mr. Vigneault was asked about a PCO intelligence assessment, referred to as the PCO Special Report. [The NSIRA Report describes the PCO Special Report as a PCO product about PRC FI requested by then-Acting National Security and Intelligence Advisor ("**Acting NSIA**"), Mr. David Morrison, in the autumn of 2021. NSIRA found that, in January 2022, under a new NSIA, Ms. Jody Thomas, the PCO's Intelligence

Assessment Secretariat ("**IAS**") recommended providing the Special Report to select DMs and Cabinet Ministers. NSIRA also found that the Special Report had remained in draft form and had not been sent to these individuals or to the Prime Minister's Office].

[39] Ms. Henderson explained that PCO IAS reached out to get CSIS' perspective and assistance on the Special Report. She noted that Mr. Morrison wanted a better appreciation of what CSIS was seeing and assessing and explained that Mr. Green [at PCO's IAS] reached out to CSIS to advise of Mr. Morrison's request and to ask for support. CSIS reviewed the paper. Ms. Henderson noted IAS also added what threats they were seeing from an international perspective. Mr. Vigneault noted that it was clear how CSIS was seeing the threat and that Mr. Morrison wanted another, "more objective" view. Mr. Vigneault indicated that this exchange did not have an impact on his or the Service's activities so he did not have any further discussions on the issue, and it was not discussed at the DM level. As it was led by IAS, they were responsible for coordinating and drafting the final product. It would not go for DM discussion until it was to be published.

6. Challenges to Detecting, Countering and Deterring FI

6.1 Resource Allocation

[40] Mr. Vigneault noted that the 2024 Federal Budget was the result of ongoing efforts by CSIS to respond to extreme pressure it experiences because of limited resources. [The Budget proposes to provide $655.7 million over eight years, with $191.1 million in remaining amortization, and $114.7 million ongoing, to CSIS to enhance its intelligence capabilities and its presence in Toronto]. Ms. Lloyd said that Service requests for increased funding began in 2023. She noted that CSIS had to make difficult choices in prioritizing its actions, a limit that some foreign threat actors do not necessarily face. Dr. Giles explained that CSIS performed an analysis to identify its biggest and most impactful legislative gaps compared to its allies. Budget 2024 was the first time that CSIS funding allocations were mentioned explicitly in a Budget, furthering transparency.

[41] Dr. Giles explained that the incremental funding was targeted to enable CSIS to pursue initiatives to enhance its intelligence capabilities and technological systems.

[42] Both Ms. Lloyd and Mr. Vigneault emphasized that the funds allocated in the 2024 Budget are for transformation, not the day-to-day work of CSIS, and that the funds will not fill every gap. Mr. Shortliffe gave the example of how the increased funding will affect collecting information pursuant to a warrant. While the resources allocated in the budget may enhance CSIS' collection capabilities, resourcing challenges remain.

6.2 Gaps in Authorities and Bill C-70

[43] The interviewees were asked about two internal documents identifying gaps in Service authorities.

[44] Dr. Giles noted that Bill C-70, *An Act Respecting countering foreign interference*,[3] was, in a way, a complement to the funding secured by CSIS in the 2024 Federal Budget. CSIS needed both new authorities and additional resources. Reflecting on the Bill, she believed that there had previously been no widespread desire to modernize the security and intelligence legislative framework. She said legislative changes in that area also required public buy-in, notably because of a general lack of public trust in the security and intelligence community and because of privacy concerns.

[45] Dr. Giles added that CSIS had established its priorities, and potential solutions, further to a consultation within CSIS writ large. This allowed it to prepare the document containing a table of gaps and develop proposals to address them. This then led to broader discussions and consultations within government to determine (i) which of these gaps were related to FI and (ii) which gaps could be addressed within a year. She noted that the limited timeframe contemplated for Bill C-70 had led CSIS to forego some more ambitious legislative proposals, including proposals about its dataset regime.

[46] Dr. Giles said the overarching goal was to determine what CSIS needed to: 1. better equip national security partners; 2. operate in a digital world; and 3. respond to evolving

[3] Bill C-70 received Royal Assent on June 20, 2024 and was enacted as *An Act Respecting countering foreign interference*, SC 2024, c 16. It modifies the *CSIS Act*, RSC 1985, c C-23.

threats; *CSIS Act* amendments contained in Bill C-70 furthered this process, addressing five core areas:

a) **Information sharing under section 19.** Dr. Giles noted that these amendments are intended to (i) build resiliency to FI throughout the Canadian population, (ii) enable FI-related investigations and prosecutions (e.g., by sharing information with provincial electoral bodies who have investigative authority), and (iii) allow for the balancing of privacy interests when disclosure is required in the public interest. She described the overarching objective of this amendment as facilitating the sharing of classified information by CSIS. Ms. Lloyd and Mr. Vigneault added that the current legal framework permitting CSIS to share classified information is multi-layered, involving multiple authorities such as s. 19 of the *CSIS Act*, s. 12 of the *CSIS Act*, Threat Reduction Measures, Ministerial Directives, and presents significant and overlapping legal risks. Mr. Fisher said that this has sometimes led CSIS to refrain from sharing information even if it believed that it had the authority to do so. For instance, CSIS might hesitate to share information when it cannot be sure that the information could later be protected if a criminal prosecution were to arise. Ms. Henderson added that, for this legislative change to produce its intended effects, the recipient must also be willing to hear the information that CSIS provides.

b) **Updates to the warrant regime**. Dr. Giles explained that obtaining warrants can be extremely resource-intensive under the current "one-size-fits-all" warrant regime. This regime requires CSIS to seek comprehensive warrants for one-off techniques. Bill C-70 will allow for single use warrants [these warrants would allow CSIS to conduct a single collection activity. Under the current regime, CSIS may only seek a broader warrant, which requires it to discharge a heavy burden]. The amendments will also allow for CSIS to seek Production Orders and Preservation Orders. She explained that the changes to the warrant regime are still subject to safeguards and Federal Court approval.

c) **Updates to the dataset provisions.** Dr. Giles explained that CSIS currently has only 90 days to receive, decrypt, and translate a dataset, as well as to isolate

data about Canadians (which is subject to a different regime under the *CSIS Act*) from the dataset and evaluate its contents before it must ask permission to retain the datasets. Bill C-70 will increase that time to 180 days. In addition, the amendments to the dataset regime clarify the uses of datasets, allow datasets to be used in immigration screening, broaden the use of datasets in exigent circumstances, allow for use of a single regime for the treatment of both foreign datasets and Canadian datasets, and amend provisions on sharing datasets.

d) **Clarify the scope of section 16 of the *CSIS Act*,**[4] Dr. Giles explained that, as currently written and interpreted by the Federal Court, section 16 of the *CSIS Act* posed some challenges, including because the activities of threat actors are often not tied to particular locations; they have components that are foreign, but other aspects may have a Canadian nexus. Dr. Giles explained that the amendments will allow CSIS to collect, from within Canada, information held outside Canada related to warranted section 16 investigations of activities inside Canada.

e) **Mandatory review of the *CSIS Act* every five years.** Mr. Vigneault noted that Bill C-70 will also require a review of the *CSIS Act* every five years. He explained that the goal is to de-politicize and de-dramatize making changes to the *Act* so that it can evolve with technological change. Mr. Vigneault noted that this speaks to a broader need to de-politicize national security.

7. Specific Incidents of FI

7.1 Update on Incident from 2021

[47] Commission counsel sought further information from the witnesses about an issue related to foreign interference that resulted in a briefing to the secret-cleared

[4] [Section 16 of the CSIS Act states that "the Service may . . . assist the Minister of National Defence or the Minister of Foreign Affairs, within Canada, in the collection of information or intelligence relating to the capabilities, intentions or activities of (a) any foreign state or group of foreign states; or (b) any person other than (i) a Canadian citizen, (ii) a permanent resident . . ., or (iii) a corporation . . ."].

representatives of the Liberal Party of Canada shortly before the 2021 election and to the Prime Minister shortly after.

7.2 Update on Don Valley North

[48] Commission Counsel sought further information on allegations of FI relating to Han Dong. This included asking whether there was any request of CSIS from the Prime Minister or his office after the 2019 election for follow up on Han Dong. Mr. Vigneault recalled that the Prime Minister was briefed in early 2023 and there was a process to brief ministers during the spring of 2023. He was not sure if any other briefings took place with the Prime Minister.

7.3 Oxford Nomination

[49] Commission counsel brought the witnesses to a document referencing open source allegations that a candidate in Oxford, Ontario was "parachuted" into the riding and that there were "nomination race irregularities." Mr. Basler remembered the incident, and the conclusion of SITE TF that it did not observe any indication of FI directed at the by-election.

7.4 Conservative Party Leadership Race

[50] Commission Counsel asked the witnesses to comment on a conclusion in the NSICOP Report that suggests foreign actors targeted party leadership campaigns and interfered in leadership races of the Conservative Party of Canada.[5] Mr. Vigneault clarified that the conclusions of the NSICOP report are stark compared with the intelligence reporting, and that the NSICOP conclusions must be nuanced in light of intelligence gaps. Mr. Basler emphasized that the conclusions drawn by NSICOP are only those of NSICOP based on the documents they received. They are not the Service's conclusions and the Service does not have fidelity on the path by NSICOP to making its conclusions.

[5] Paras 72-73.

8. Tools to Counter FI

8.1 Identifying Vulnerable MPs and Ridings

[51] Commission Counsel asked the witnesses about a working document drafted before the 2021 federal election. The document sets out a methodology for identifying potentially vulnerable nomination races. Mr. Basler explained that he did not believe this document went up to the executive level, but that it appeared to reflect an ongoing discussion regarding the Service's efforts to identify MPs who are higher risk. Mr. Shortliffe remembered seeing the list of vulnerable nomination races. He explained that this type of document would be used as an investigative tool by the regions to help determine where to look and which questions to ask. Ms. Henderson agreed that this type of document would help inform operational work.

[52] Mr. Vigneault explained that the Service's approach to identifying vulnerable ridings is evolving and that the Service is trying to identify tools or analysis that could be useful in future. Ms. Lloyd agreed that they had been thinking about this type of analysis but that she does not expect that the relevant factors considered by threat actors to choose their targets for influence will change significantly.

[53] Mr. Basler further explained that during the by-elections beginning in June 2023, the Service's analytical resources were put towards compiling baseline assessments of the four election ridings. CSIS has been considering how to do something similar in the next general election as these are well received by the Panel of Five and the Deputy Ministers' Committee for Intelligence Response.[6] He noted that CSIS' limited resources must be considered in determining the approach for the general election.

8.2 The SITE TF

[54] Dr. Giles noted that the future of the SITE TF has been an ongoing discussion. The SITE TF was only intended to be active during the writ period. However, this approach

[6] The Deputy Ministers' Committee on Intelligence Response is meant to identify relevant actionable intelligence, make coordinated decisions on how to best respond with operational, enforcement, or policy action, and triage the intelligence to be briefed to Cabinet and the Prime Minster.

does not account for the fact that threats exist outside the writ period. She also noted the challenges with having a rotating chair and membership turnover, including a lack of institutional memory, and the difficulty of building and maintaining trust with political parties. She suggested that the SITE TF be permanent and centralized, with a consistent chair and secretariat. However, there is ongoing discussion about where to house the SITE TF and who should assume the permanent chair. She noted that there could be concerns with housing the SITE TF too close to the center [PCO], given is proximity to the political level. She said, however, that governance and coordination on national security, as with other topics, there is value in proximity.

[55] Mr. Vigneault added that we should be careful not to silo or duplicate groups working on the same issue, for example, if the SITE TF is housed at PCO while the FI coordinator role remains housed at Public Safety. There needs to be an organized approach to FI writ large, rather than "siloing" different groups, leading them to look at FI only in certain circumstances, such as elections. He noted that the SITE TF might not be the appropriate conduit to approach and tackle broader FI issues including mis- and dis-information, threats to diaspora groups, and others.

[56] Mr. Basler said the SITE TF currently works well during an election but does not address the full threat of FI. Much of what happens in FI occurs before the election, so focusing only on the writ period is too limited. The baseline assessments during the by-elections demonstrate the need for a broader assessment of the threat. Dr. Giles noted that even if the SITE TF were to be permanent, separate protocols would still be necessary for when the writ drops.

8.3 Proposed TRM

[57] Commission Counsel showed the witnesses an email thread about a proposed TRM to respond to an FI threat. Mr. Shortliffe explained that the impetus for the TRM was to sensitize politicians and people working in government to the potential FI threat. Mr. Shortliffe noted that there is a robust process for assessing the risk of TRMs. He reviewed the proposed TRM and was concerned about the potential risk of the specific details of the TRM becoming public.

[58] Consideration was then given to the extent to which a TRM was necessary to achieve the Service's objectives. Parts of the TRM could be executed under the Service's mandate without a TRM. In Mr. Shortliffe's view, implementation of these aspects would allow the Service to reduce the threat while avoiding the risks inherent in other aspects of the proposal.

[59] Ms. Henderson added that during the discussions about the TRM, other events diminished the need for it.

8.4 Engagement with Michael Chong

[60] Commission Counsel asked the witnesses about a document listing CSIS' engagement with Michael Chong and related discussions.[7] Mr. Basler confirmed that he believed the list was accurate as his team created it and that it had likely been prepared for PCO in light of the media leaks. CSIS' practice with engagements such as this is to explain that it will keep the conversation, and any information it might be given, confidential. In addition, CSIS will explain that the individual is also expected to keep the conversation confidential, although maintaining confidentiality is not legally required.

9. Engagement with Diasporas

[61] Mr. Ouellette explained that CSIS has four pillars in terms of its academic engagement and outreach program: (1) research/academia; (2) industry; (3) Indigenous partnerships; and (4) community advocacy associations, including diaspora communities. For diaspora communities, CSIS headquarters focuses on engagement with national organizations. The program seeks to help explain to diaspora groups what CSIS does, build trust with the organizations and those they represent, and build a culture of national security in the wider Canadian community and outside the federal government.

[62] Dr. Giles explained that engaging with diaspora organizations is not necessarily straightforward. It may take numerous calls, emails, and meetings before a meaningful relationship begins and real dialogue can ensue.

---

[7] CAN013134.

[63] Dr. Giles stressed the importance of ongoing engagement with organizations. This can take a lot of energy. She also emphasized that CSIS has to listen and adapt. For instance, she heard from various groups that they do not like the term "diaspora", as they feel it differentiates them from other Canadians; CSIS adjusted the language used when engaging with those groups.

[64] Both Dr. Giles and Mr. Ouellette also spoke about the need to address concerns about racism within CSIS itself as well as within the public service and greater Canadian society. Dr. Giles gave the examples of a Trust Pamphlet, a publication which engages issues of racism and CSIS, and the Cross-Cultural Roundtable on Security visit to CSIS Headquarters, where the Assistant Director of Human Resources at CSIS explained the vision for CSIS and sought to have conversations on reconciliation, diversity, equity and inclusion. They explained that this engagement and atonement for the past is necessary to reconcile and build trust with communities.

[65] Mr. Vigneault noted that in the past, national security has been portrayed as zero-sum, civil liberties versus "Big Brother," a proposition he challenges. Mr. Ouellette added that they have noticed a shift in how diaspora communities and civil liberties organizations view national security. He gave the example of Bill C-70. Before CSIS' work on outreach, the Service would have expected certain groups to be fully opposed to any expansion of CSIS authority. However, rather than expressing immediate and vigorous opposition, such organizations offered a more nuanced response, only requesting more time to evaluate. This is viewed as a success.

[66] From an operational point of view, Mr. Basler added that relationships with communities is critical for the Service's understanding of, and reporting on, foreign interference.