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

In Camera Examination Summary: Canadian Security Intelligence Service Senior Officials

Commission Counsel examined senior officials from the Canadian Security Intelligence Service ("**CSIS**" or the "**Service**") during *in camera* hearings held in July and August 2024. This is a summary of the testimony given in July. Counsel for the Attorney General of Canada appeared on behalf of the Government of Canada and had the opportunity to examine the witnesses. The hearing was held in the absence of the public and other Participants. This summary discloses the evidence that, in the opinion of the Commissioner, would not be injurious to 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. Witnesses

[1] David Vigneault was Director of CSIS from June 2017 to July 2024.

[2] Vanessa Lloyd was appointed Interim Director of CSIS in July 2024 and is concurrently its Deputy Director of Operations ("**DDO**"). She was appointed to that position in May 2023. From 2020 to her appointment as DDO, she held a senior executive position at CSIS focused on modernization of the Service's operational capabilities and methodology.

[3] Michelle Tessier was the DDO for CSIS from December 2018 until March 2023. She worked for the Service for 35 years and is now retired.

[4] Bo Basler is Director General of the CSIS Counter-Foreign Interference Tiger Team and the Counter-Foreign Interference Coordinator for the Service. He has held this position

since March 2023. Prior to that, he served as a Regional Director General and Regional Deputy Director General.

[5] Newton Shortliffe was the Assistant Director of Collection ("**ADC**") for CSIS. He became acting ADC in 2021 and permanent ADC in 2022. The ADC is responsible for the collection of intelligence for all regions. He is now retired.

[6] Adam Fisher has been Director General of the Litigation and Disclosure Branch at CSIS since the autumn of 2023. The Branch is responsible for managing litigation processes as it pertains to civil and criminal litigation and the Branch's Access to Information Unit.

2. Examination by Commission Counsel

[7] Mr. Vigneault confirmed that he had read the classified CSIS Stage 2 Institutional Report ("**Classified CSIS IR**"), that it was accurate to the best of his knowledge and that he was content that it be filed as part of CSIS' evidence before the Commission.

2.1 Current Threat Landscape

2.1.1 China

[8] Commission Counsel asked about the threat landscape as it stands today. Mr. Vigneault stated that the People's Republic of China (**"PRC"**) represents a multi-vector threat. Its approach is centralized by the Chinese Communist Party ("**CCP**") directed by Xi Jinping and involves the entire Chinese state apparatus. The ultimate goal is to ensure the survival of the CCP. Economic, military and cultural activities of the PRC are all directed towards this goal. Some activities are benign while others are malicious and can take the form of threats or confrontation with the interests of Canada and its allies.

[9] Mr. Vigneault stated that since Xi Jinping took power in 2012 there has been an expansion in the power of the CCP and a specific goal of military dominance. Everything that occurs in the economy is overseen by a committee presided by Xi Jinping. The PRC has also passed coercive national security laws that reach across the globe to control all individuals of Chinese origin. These laws also have an impact on the

activities conducted by foreigners in China. There is a hardening of the position taken by the PRC and of the threat posed by the country as a result.

2.1.2 India

[10] Mr. Vigneault testified that India generally has friendly relations with Canada. However, there has been a significant increase in Indian nationalism and a desire to develop state tools, including cyber tools, to project and pursue India's interests abroad. India has a very strong technology-based economy and also relies on technology provided by other states and companies to pursue its interests.

[11] Mr. Vigneault stated that, historically, India was the largest and most important of the non-aligned states during the Cold War. Under Prime Minister Modi, geopolitical conflicts between India and China have increased.

2.1.3 Russia

[12] Commission Counsel asked about Russia's covert operations in the information space aimed at eroding the values of liberal democracies. Mr. Vigneault referred to his previous testimony before the Commission in which he stated that even though Russia has the capacity to interfere in the elections of democratic states, CSIS has not seen it happen in Canada. However, one of Russia's main objectives is to weaken liberal democracies around the world. One method used by Russia is to amplify societal divisions. The tools it uses in pursuing that goal include social media, disinformation and co-opting journalists directly to create divisions in western democracies that will benefit Russian interests. Unlike Canada, Russia's actions are not constrained by the rule of law and the *Charter*.

[13] In Canada, this strategy can take the form of trying to portray authoritarian regimes in a more positive light than democracies. Canada has seen few such attacks, but it happened with the recent French elections.

[14] Mr. Vigneault stated that, like China, Russia takes coordinated state action to accomplish its goals. Russian oligarchs and large Russian companies are put to service

in this process. Both in Russia and China, criminal groups are involved in activities such as cyberattacks or ransomware. Criminal groups can be used to carry out measures that are not directly attributable to a government so tend to disguise the government's involvement. Mr. Vigneault gave an example where Russia was warned against using such tactics in Canada.

[15] Mr. Vigneault stated that the last two to three years have seen a significant increase in the number of countries using criminal groups for state purposes.

[16] Ms. Tessier described Russia's covert operations in the information space as a psychological war. Russia's goal is to undermine Western government's credibility and uses criminal groups to attack critical infrastructure. This undermines the confidence citizens have in their government's ability to manage crises.

[17] Ms. Lloyd stated that the Service is paying great attention to what it is calling "the year of the elections". This means a lot of engagement with counterpart services, particularly in Europe because of elections in Eastern Europe – last year in Poland – and this year in the UK and France. There is already open-source analysis about how much Russia has engaged in mis- and disinformation using artificial intelligence and bots. CSIS will engage with partners to better understand Russia's tactics, because the level of Russian interest in Canadian democratic processes is lower. Ms. Lloyd stated that this sharing of information allows CSIS to understand the tactics and interests of an adversary at a specific point in time. For instance, in the federal elections of 2019 and 2021, Russia's engagement was perhaps less because of the nature of Canada's engagement on issues of concern to Russia. Since then, Canada has come out quite strongly in support of Ukraine. Whether that changes how much Russia would want to influence the next election will likely depend on the level of investment that Russia wishes to make against Canadian positions and affairs. In general, the level of intensity of threats from hostile state actors depends simultaneously on what the hostile state itself is trying to achieve on the global stage, and on bilateral relations between Canada and that hostile state.

[18] Mr. Vigneault noted that after the invasion of Crimea in 2014, Canada decided to unilaterally withdraw a number of Canadian diplomats from Russia to protest the

invasion. Canada did not reduce the number of Russian diplomats in Canada. However, after the Russian attack on a former Russian spy in the UK, Mr. Skripal, Canada declared four Russians *persona non grata* ("**PNG**"). Russia then declared four Canadian diplomats PNG. This resulted in a much lower number of Canadian diplomats in Russia than Russian diplomats in Canada. Such expulsions are one of the important tools available to governments to send messages to other governments.

[19] Ms. Lloyd stated that Russia, China and India conduct foreign interference activities through foreign state officials in Canada and proxies. Ms. Lloyd discussed how the Service collects intelligence on these activities.

2.1.4 Iran

[20] Iran relies on criminal groups, criminal plots, assassinations and kidnappings. For example, criminal charges in the US have been laid against criminals, including Hells Angels affiliates in Canada, for actions they undertook on behalf of Iran in its plots against Iranian dissidents. Iran employs psychological harassment on social media, communicates with family members and uses criminal groups and other proxies.

[21] Ms. Lloyd stated that the Government has recently decided to list the Islamic Revolutionary Guard Corps as a terrorist entity in Canada. The Iranian government could directly respond to that decision or it might increase its FI activities leading up to an election. Iran, among others, has a common focus on transnational repression of diaspora groups. Determining whether these tactics prevent a community from participating in a democratic process is difficult for an intelligence service like CSIS to assess, unlike its ability to observe direct activity by hostile state actors to interfere in a democratic process, for example, when they attempt to influence the nomination of candidates. The activities of these countries are quite different from those of Russia, China, and India.

2.1.5 Other Countries

[22] Ms. Lloyd and Mr. Vigneault testified about the Service's observation of foreign interference by other countries, including Pakistan. They described Pakistan as fairly opportunistic and noted that Pakistan's foreign interference against Canada must be viewed through the Pakistan-India prism. They also commented on the activities of other countries, which focus primarily on transnational repression.

[23] Many governments might target political opponents in Canada, but not all instances are investigated by the Service. Resources are a consideration.

2.1.6 Impact on Diasporas

[24] Mr. Vigneault noted that people from other countries come to Canada to benefit from Canada's protection of rights. However, sometimes their countries of origin continue to harass them here. Many countries consider it legitimate to ask Canada to do something to stop their dissidents who reside in Canada. This has created very difficult moments with allies. Countries may say it is an affront for Canada to allow demonstrations against them when their leaders visit Canada. Canada's response is that this is Canadian democracy; this is what it is like here. This dynamic is very important in the discussion of FI against dissidents. FI is notably different in the case of countries like China, Russia and India that now have greatly increased FI capacity and intensity.

2.2 CSIS Security Alerts

[25] Commission Counsel asked for an explanation of "security alerts" and when they are used. Ms. Lloyd said that before Bill C-70 became law, CSIS had challenges in sharing information with the public to increase resilience. One tool CSIS developed was the security alert. CSIS uses information to make a statement that does not jeopardize the security of operations, sources, methodologies or classified holdings. The statement can still make the point that an activity is happening that the Canadian public should know about. Canada may do this with Five Eyes partners in a campaign approach to mitigate the effects of a particular threat activity more broadly.

[26] Ms. Lloyd gave the example of a security alert about activities by a hostile state using a transnational organized crime group as a proxy. An alert could also increase awareness that something exists and could be used as a vector by a hostile state actor to conduct threat activity in Canada.

[27] Mr. Vigneault stated that a number of tools – for instance, Threat Reduction Measures ("**TRMs**") – exist to reduce threats. The challenge is in determining how CSIS can reduce the impact of FI operations in Canada in accordance with the *CSIS Act*. Mr. Vigneault gave an example of a security alert unrelated to Canada's electoral processes and democratic institutions.

[28] Mr. Vigneault recalled that CSIS had issued a security alert recommending caution to a provincial government in the use of particular PRC-manufactured technology. PRC law obliges Chinese companies to share information obtained through such technologies with the PRC government.

2.3 Significant Instances of Suspected Foreign Interference[1]

[29] Mr. Vigneault testified about the significant instances of suspected FI described in the Classified CSIS IR. [Page 2 of the Classified CSIS IR states: "To determine the most

[1] The Classified CSIS Stage 2 Institutional Report delivered to the Commission on July 8, 2024 contained a list of significant instances of suspected foreign interference created at the request of the Commission. In early September 2024, CSIS informed the Commission that it had reassessed one instance which related to a specific parliamentarian, in light of additional information. On September 5 2024, CSIS undertook a review of public records related to the instance. In the course of this review, CSIS learned information that directly contradicted a significant element of the instance as described in the Classified CSIS IR and the CSIS reporting on which it was based. Since the parliamentarian was not a subject or focus of any investigation, CSIS had not tracked the publicly available information regarding the instance.

According to CSIS, this additional information revealed that this instance had a lesser impact on Canada's democratic processes than CSIS previously understood. CSIS continues to view this as a suspected instance of foreign interference as it demonstrated a foreign government attempting to build, maintain or leverage relationships with parliamentarians using clandestine, deceptive or threatening tactics as defined in the *CSIS Act*. However, CSIS now assesses that this instance is not of the same order of magnitude as other instances listed in the Classified CSIS IR, as the activity did not have the outcome intended by the foreign government. CSIS relayed this reassessment to PCO, including the National Security and Intelligence Advisor

significant instances, factors such as potential for actual impact on democratic processes, potential to undermine public confidence or the knowing participation of a parliamentarian, were considered. In each case there needed to be an element of clandestine, covert or threatening behavior by the foreign state actor involved." An explanation of how the Government created the list of these instances can be found at pages 1 and 2 of the unclassified CSIS Stage 2 Institutional Report.] These were selected by consensus among several government departments and agencies (the Privy Council Office ("**PCO**"), GAC, the Communication Security Establishment ("**CSE**") and CSIS). He noted that organizations might individually differ in their assessment of the importance of particular incidents.

[30] For CSIS, section 2(b) of the *CSIS Act* is very clear about what activity constitutes FI. This definition dictates the Service's operations and analysis. For the purposes of their investigative work, it is very clear: if there is threat activity that meets the threshold of section 2(b), they can investigate. Things may be very different if the situation is looked at from another perspective. In some cases there is no ambiguity; all the components of FI are present. In other cases, all the components of foreign influence are present yet the activity is normal diplomacy. A grey zone exists between the two. The knowledge that the PRC has a clear desire to interfere in Canada by all possible means allows CSIS to characterize a particular PRC activity (which might otherwise fall into the grey zone) as likely FI, and not simply foreign influence. Particular actions of the PRC may look like foreign influence, but CSIS views them differently in light of the broader context of the PRC's intentions. Another organization may have a different view. For this reason, discussions around the table are very dynamic.

[31] Mr. Vigneault said that there has been a very important evolution over time regarding the different perspectives on what constitutes FI. Three or four years ago, these differences were greater because there was less discussion and there were fewer

---

("NSIA"). The NSIA agreed that, in light of this information, the instance should no longer be included in this list. Further consultation across senior government officials resulted in affirmation of this decision. Given the reassessment, CSIS has amended the Classified CSIS IR to remove this item from the list of significant instances.

engagements on the subject. A tension between the perspectives remains in some cases, but the nuances are much more precise than before. This allows for more frank discussions, although there will not necessarily be agreement on everything. Mr. Vigneault believes that in a democracy, it is healthy that an intelligence service not have the last word on everything. Still, it is necessary for the Service to be at the table to ensure its perspective is well represented. Mr. Vigneault stated that CSIS has been investigating FI since 1984. It is much more difficult for police forces to do so since they have many other priorities. However, the operational perspective has significantly evolved over the past two years or so. This is one of the main reasons the Government made changes to the *Criminal Code* and the *Security of Information Act* [in Bill C-70] – to more precisely identify the illegal activity related to FI that police forces can investigate.

[32] Mr. Vigneault said that there are fewer differing perspectives of FI among organizations and that the public discussion on FI contributed to this evolution. Government organizations are now able to have much more frank discussions about whether an organization can take action on a particular situation. The PRC police stations are a good example. CSIS led the inquiry at the start and the RCMP took over later.

[33] Mr. Vigneault spoke of a difference in perspectives that may have existed in the past between the Service and political actors in Government concerning certain aspects of the political process, such as nomination processes. He noted that these differences came to light in the Commission's public hearings. Mr. Vigneault noted that they are much less now and there is a much better understanding on both sides. This helps him in determining how to brief Government. He now briefs differently, including by being more precise about the links between the subject-matter of the briefing and the *CSIS Act*. He also noted that he receives a very high level of support from the Minister of Public Safety.

[34] Ms. Tessier stated that Canada does not have a strong intelligence culture. There is a lack of understanding of intelligence at all levels. The work of this Commission is very important since people are becoming much more interested and are trying to understand the national security space. Ms. Tessier testified that FI generally unfolds

over a long period of time. When a government client receives a discrete piece of intelligence, the feedback they can provide to CSIS is important because it improves not only the intelligence collection and its assessment, but also the understanding of the recipients of the intelligence.

2.4 Specific FI Incidents

2.4.1 Update on Incident from 2021

[35] The witnesses were asked about and provided further evidence about an issue related to foreign interference that resulted in a briefing to the secret-cleared representatives of the Liberal Party of Canada shortly before the 2021 election and to the Prime Minister shortly after.

2.4.2 Update on Don Valley North

[36] The witnesses responded to questions from Commission counsel regarding further information on allegations of foreign interference relating to Han Dong. This included testimony that, following the media leaks in 2023, a process was put in place to brief certain ministers. Mr. Vigneault also noted that all requests from the PM to CSIS come via the National Security and Intelligence Advisor **("NSIA")** Office in PCO.

2.4.3 Government of India Financial Support

[37] The witnesses testified about a body of intelligence that indicates that the Government of India leveraged a proxy agent to clandestinely provide financial support to Canadian politicians from three federal political parties in a federal election. Whether the candidates received the funds or knew of their origins cannot be confirmed.

2.4.4 Nijjar Murder and Indian FI

[38] The witnesses testified about the evolution in their understanding of the Government of India's possible involvement in the Nijjar murder. CSIS prepared various assessments

in relation to this matter. Once Mr. Vigneault was convinced there was Indian involvement, he briefed Jody Thomas [the NSIA at the time] and they briefed the PM.

[39] Before the 2023 G-20 meeting, Mr. Vigneault met with security and intelligence counterparts. He explained to the Commission that service-to-service talks occur regularly and it is possible for them to have frank discussions.

2.4.5 Overseas Police Stations

[40] Mr. Vigneault said that the use of community organizations integrated into the diaspora community as a tool of transnational repression is a known tactic of the PRC and another example of the PRC's approach to FI. While this activity can provide useful services to diaspora members, it remains contrary to Canada's interests.

[41] CSIS shared information with the RCMP pertaining to overseas police stations.

[42] Ms. Tessier stated that in many cases these stations are managed by Canadian citizens, not diplomats or foreigners, thereby limiting the ways in which Canada can respond. They may not be police stations as such, but rather stores or associations that offer services to the Chinese community.

2.5 Challenges to the Collection and Sharing of Intelligence

[43] Ms. Tessier discussed the challenges surrounding intelligence gaps. One of the first things an intelligence service attempts to do is corroborate the information it receives, but it is sometimes very difficult or even impossible to do so. One gap which Bill C-70 may help address is the capacity of CSIS to search, analyze and conserve data. The ability to search in a wide variety of databases, for instance, – is very important. But there will always be cases where intelligence cannot be fully corroborated. There is a need to modernize the tools available in CSIS' toolkit.

[44] Mr. Vigneault added that beyond allowing CSIS to obtain information for analysis is the ability to share information so others can meaningfully use it – the Commissioner of Canada Elections, for example. In some cases, the information might be Top Secret or

Special Access. Using this kind of information becomes very complicated and it's part of the 'intelligence-to-evidence' issue.

[45] Mr. Vigneault noted that while CSIS sometimes has sufficient intelligence to confidently determine what is happening, other times CSIS may need to ask a partner department or agency to use its mandate to complete the picture. He stated that CSIS needs both to receive and analyze the right information, as Ms. Tessier noted, and then be able to share this information at the right time so that others can make good use of it.

[46] Ms. Lloyd noted that the passage of Bill C-70 means that the *CSIS Act* will have to be reviewed every five years. This is a very positive step. Other changes to the *CSIS Act* have been helpful. The coming period of using those newer authorities will show whether changes to the *CSIS Act* alone are sufficient. A prior change to legislation, in this example the *Security of Canada Information Disclosure Act*, gave CSIS permission to ask departments for disclosure of information, but did not necessarily give the departments clear permission to disclose. Once CSIS builds its experience with these new authorities, it will be in a position to provide feedback, or perhaps a review more broadly of national security legislation would help solve some intelligence-to-evidence challenges.

[47] Ms. Lloyd stated that the safety of human sources is a consideration in investigative steps and weighs very heavily on those responsible for CSIS operations – to act ethically with those who collaborate in maintaining the safety and security of Canada.

[48] Ms. Lloyd stated that CSIS may also come to a point in an investigation where it is unclear about the awareness of the parties involved. Going directly to an individual to gain this clarity and share information that the Service knows it not without risk.

2.6 CSIS Counter Foreign Interference Tiger Team

[49] Mr. Basler, Director General of the CSIS Counter Foreign Interference Tiger Team, explained that the Tiger Team was created about 15 months ago to respond to an unprecedented number of demands from within government about foreign interference. Coordinating the response was having a significant impact on the operational branches

of the Service. CSIS senior executives at that moment decided to create a Tiger Team to respond and to address all policy and relationship-building aspects of the FI issue housed within a dedicated section of the Service. It would also respond to the demands stemming from reviews by the National Security and Intelligence Committee of Parliamentarians ("**NSICOP**"), the National Security and Intelligence Review Agency ("**NSIRA**"), the Independent Special Rapporteur and the Commission. The Tiger Team also houses the SITE Task Force.

[50] Mr. Basler testified that he has consistent communication with the Public Safety Counter-Foreign Interference Coordinator. During the recent briefings to parliamentarians, done caucus by caucus, Mr. Basler's team worked with the PS Coordinator. Mr. Basler said that his unit and the PS Coordinator work together on issues of common interest as they come up.

2.7 Additional Information on the CSIS Stage 2 Institutional Report

[51] Mr. Basler explained the development of the list of significant instances of suspected FI following a request made by the Commission. Mr. Basler explained that, to identify these seven significant instances of FI, CSIS triaged the intelligence products it had disseminated to other government departments and agencies, and produced an initial list of potential instances. The final list of seven significant instances was determined in consultation with all engaged agencies.

[52] Commission counsel asked the witnesses a series of questions about instances in the Classified CSIS IR which correspond to bullet points number one, two, and six of the unclassified CSIS Stage 2 Institutional Report.

2.8 The "Targeting Paper"

[53] The witnesses were invited to discuss a 2021 document, sometimes referred to as the "Targeting Paper," published in 2023. Ms. Tessier explained that "targeting" in this context means someone the PRC is looking to influence. It does not imply that the

"targets" are complicit; nor does it imply that they are threatened in any way. The Targeting Paper was meant to identify how and why the PRC targets individuals, more specifically, parliamentarians. [The Targeting Paper was initially prepared in 2021. It was not published or disseminated at that time; however, it was circulated to a small number of senior officials. It was published in SLINGSHOT on February 13, 2023 and seen by approximately 40 public servants before it was made inaccessible on February 22, 2023.]

[54] Mr. Vigneault testified that an initial version of the Targeting Paper was discussed during a meeting [on February 24, 2023] between Mr. Vigneault, the NSIA and various deputy ministers, including the Public Safety Deputy Minister and the Foreign Affairs Deputy Minister. The highly sensitive nature of the information contained in the Targeting Paper was discussed during that meeting; the paper named various targeted parliamentarians. A request was made to CSIS to review and transform the document so that it could be more broadly disseminated. Mr. Vigneault saw no issue with that request. It took a long time to complete the paper due to some confusion between CSIS and PCO with respect to tasking. Upon learning that the paper was not completed, he requested that it be finalized as soon as possible. Mr. Vigneault understood that a less sensitive version would be distributed.

[55] Several months later, Mr. Vigneault was very surprised to learn, during a review conducted by NSIRA, that the less sensitive version of the Targeting Paper was never distributed to the PM. Mr. Vigneault understood from the NSIRA or NSICOP final report that the then-NSIA Jody Thomas had decided not to share the paper with the PM because it was determined that the conduct described therein was more diplomatic than it was FI. This surprised him. He could not speculate on why such a decision would have been made, but he found the paper very pertinent. He thought it should have been distributed but the NSIA had not discussed it with him nor had she asked for his opinion. The source of his understanding that the NSIA had decided not to share the paper was the NSICOP and NSIRA reports, not personal knowledge.

[56] Mr. Vigneault stated that at that time, there was no formal system to meet and discuss. Governance has now changed and meetings occur every two weeks to discuss reports.

It is the proper role of the NSIA to decide which of the hundreds of reports produced by CSIS each year go to the PM. Nevertheless, it is important for agencies like CSIS to understand what goes to the PM and to have the PM's feedback so CSIS can improve its work. The relationship between the Service and the office of the NSIA needs to be dynamic. Mr. Vigneault believes that this relationship is now headed in the right direction.

[57] If the PM were to be briefed on intelligence, Mr. Vigneault said he would be surprised if the PM stated that he did not consider this intelligence to be indicative of FI. If this were to happen, Mr. Vigneault would want to discuss with the PM to understand why he disagreed with CSIS' conclusion that the threshold for FI had been met.

[58] Mr. Vigneault testified that the Targeting Paper would have been for the PM's information only, not for any particular action. Its goal was to generate a discussion between the PM, the Service, the PM's political advisers, and the NSIA. It is not possible for the PM to read all CSIS reports so this document was intended to provide an analysis of CSIS' holdings to facilitate discussion on the subject.

[59] With respect to distributing this version of the Targeting Paper, Mr. Basler explained that CSIS was responsible for giving CSE a list of recipients for the Targeting Paper. CSE would then distribute it over their system. The list of recipients was not determined by the CSIS analyst but it was the analyst's job to share the list with CSE, who would then distribute it. Mr. Basler agreed that it seemed that the list, which was supposed to be provided by the NSIA and CSIS Director's office, fell through the cracks.

2.9 The "PCO Special Report"

[60] Mr. Vigneault understood that when David Morrison became Acting NSIA, he asked the PCO Intelligence Assessment Secretariat ("**IAS**") to create an objective assessment of the information that CSIS had provided about PRC FI. Some back and forth occurred between PCO and CSIS during the report's preparation. He understood that PCO finalized the report and sent it to the Acting NSIA. Mr. Vigneault saw the report only in

preparation for his appearances before the Commission. The report had not been distributed to or discussed within the wider intelligence community.

2.10 The use of Intelligence Related to Foreign Interference and Political Processes

[61] Ms. Lloyd was presented with notes for a SITE briefing of the Panel of Five dated March 25, 2024 that discussed intelligence regarding alleged foreign interference directed at an opposition party aimed at influencing political processes.

[62] Mr. Vigneault said that intelligence is not evidence and noted that the law limits the information CSIS shares with others. There are several considerations when deciding whether information can be passed to someone who can act on it. When intelligence involves a politician, Mr. Vigneault explained that it may be possible to share classified information with party leaders even when this information cannot be shared with the person in question. Party leaders can take action to reduce the impact of FI. For instance, they can expel individuals from caucus and can remove some of their responsibilities.

[63] Mr. Vigneault noted that the Canadian system has not yet found an optimal way of identifying the types of information that can lead to concrete action. While the political party in government receives intelligence, it is not always clear what they can do with that information. This is even more difficult in the context of intelligence regarding opposition parties. Mr. Vigneault hopes that the Commission can provide considerations or solutions for these problems.

[64] Mr. Vigneault noted that it would not be possible or desirable in a democratic society for an intelligence agency such as CSIS to be involved in nomination processes at all levels. That said, if the nomination process rules changed or became more transparent it would be more difficult for a foreign state to interfere therein. A change in these rules would force a state like the PRC to deploy greater resources to achieve its goals.

[65] Mr. Vigneault said that it is desirable to harden the target – make Canada more resilient against the threat in order to better protect Canadian elections. Mr. Vigneault noted that

exchanging information with the election commissioners could lead to more concrete actions. There are improvements in governance, such as DMCIR where action can now regularly be discussed amongst departments, which is good since the Canadian system has not always been effective at dissuading FI because those who are caught engaging in FI are not being dealt with.

[66] Mr. Vigneault said that intelligence should be the starting point for others to inquire further. It is extremely important to ensure that the 'intelligence-to-evidence' problem is solved so that intelligence can be used as a basis for other agencies to exercise their own mandates. For example, Elections Canada or Canada Revenue Agency ("**CRA**") ought to be able to use CSIS intelligence, while protecting it, to steer their work of meeting their own legal thresholds to act. Similarly, CSIS would ideally be able to give financial information to CRA, which could then do its own investigation of an organization, for instance a charitable organization potentially being used to channel funds on behalf of a foreign state. In this hypothetical case, if the CRA found evidence of such behaviour, it could act by cancelling the organization's charitable status. Consequently, people would no longer receive tax receipts and thus would not donate to the organization and it would lose its veneer of respectability. This would diminish the organization's ability to engage in FI.

[67] With respect to solutions to FI activity, Mr. Vigneault said that some of the best solutions will come from those who are targeted by FI, who know the milieu, the ecosystem, and the types of FI that might be occurring.

[68] Ms. Lloyd stated that until Bill C-70 became law, CSIS was restricted in terms of its ability to share information outside of government. There have recently been briefings to the respective party caucuses. In some cases, protective security briefs to individuals are used to notify them that they may have been targeted. Ms. Lloyd said that CSIS officials have spent a fair amount of time speaking to counterparts and learning from allied services about how they go about disclosing information with opposition parties, amongst other things. The authorities provided by Bill C-70 also enable CSIS to look at that question differently.

[69] Mr. Shortliffe said that CSIS started a program before the 2021 election of providing protective security briefings to MPs. These were unclassified and delivered mostly by the CSIS regional offices. CSIS also had discussions about briefing the electoral district associations ("**EDAs**") because of the vulnerability of the nomination processes to FI. Mr. Shortliffe said Bill C-70 would help CSIS, for instance, by allowing them to deliver more classified briefings to organizations like EDAs, that aren't considered part of the federal government. Prior to the adoption of Bill C-70, CSIS could not, even at the federal level, give EDAs any kind of classified briefing unless doing so fell under another aspect of their authority, such as their authority with respect to TRMs.

[70] Mr. Shortliffe said that much work is still required on the intelligence-to-evidence question. Many challenges exist in providing intelligence that law enforcement and other partners can use effectively in court proceedings, for example.

2.11 FI Activities in a Leadership Contest

[71] Witnesses discussed a National Security Assessment dated October 31, 2022, which indicate that the Government of India had engaged in FI activities related to the leadership race for a political party in Canada.

[72] This included discussion of whether or not there were political party preferences among foreign states, and if so, what they were.

2.12 A Warrant

[73] Commission counsel asked Ms. Tessier about internal CSIS emails relating to this warrant and she noted that CSIS ensured the Minister's office, primarily his chief of staff Zita Astravas, would be briefed before the warrant was submitted to the Minister for approval. A briefing was held with Ms. Astravas and others approximately two weeks after the application was provided to the Minister's office.

[74] Ms. Tessier was not under the impression that the warrant would be stalled until questions that arose at the briefing were answered. It was Ms. Tessier's interpretation in speaking with Ms. Astravas that the warrant was moving ahead. There was never any

indication that Ms. Astravas would not put the warrant application to the Minister until CSIS had answered her questions.

[75] Mr. Vigneault spoke of a meeting approximately 5 weeks later with Minister Blair's office where the warrant was discussed. Minister Blair did not demonstrate or express any hesitation in signing the warrant when it was presented to him approximately one week later.

[76] Ms. Tessier stated that the CSIS regional office, headquarters, the operational employees were very frustrated with what they perceived as a delay in obtaining the Minister's approval for this warrant. It would have been the norm for the CSIS branch responsible for warrants to communicate at least verbally with Public Safety about the warrant. She could not confirm whether this happened in this case. Ms. Lloyd confirmed that it would be the norm. She noted the CSIS warrant team reported to her that they were engaging in regular administrative follow-up. There is no information in CSIS holdings that the Service was waiting for questions that it should be answering. It was really procedural.

[77] Mr. Vigneault commented on notes prepared in advance of his briefing to the Minister. He knew there were delays but no issues had been brought to his attention from Ms. Astravas, the Minister's office or his own team. For this reason he was comfortable letting things play out. He was comfortable with the timeline, and the briefing to Minister Blair reflected that. He also trusted the CSIS employees interacting with Public Safety. He was not generally the person corresponding with the Minister's office. The file was also not something that he followed daily. Mr. Vigneault's recollection is that Minister Blair was convinced by the information. He did not recall any concern about delays and he did not raise any such concern.

[78] Ms. Tessier said that in her discussions with Ms. Astravas she never had the impression that Ms. Astravas wanted to sit on the warrant or delay the application. Mr. Vigneault noted that Ms. Astravas was forthcoming and transparent in all discussions relating to the warrant. Ms. Tessier said that she always had the impression that the Minister's office was ready to proceed. She was perhaps frustrated by the delay, but not alarmed by it.

[79] The witnesses discussed different models of warrant approval processes. They noted that in some jurisdictions warrants may be approved by the director of the intelligence service and in others ministerial approval is not required.

[80] Ms. Lloyd said CSIS often discusses other models with allies to better understand their approaches. In some systems, security service laws require agencies to provide briefings under particular circumstances. Sometimes briefings on intelligence are anonymized. The Service is starting to execute on its new authorities to share classified information and is looking at ways it can evolve.