



## *In Camera* Examination Summary re: NSICOP Report: David Vigneault, Michelle Tessier, Cherie Henderson, Vanessa Lloyd, Bo Basler

Commission Counsel examined senior officials from the Canadian Security Intelligence Service (“**CSIS**” or “**the Service**”) regarding certain allegations and assertions in the National Security and Intelligence Committee of Parliamentarians’ Special Report on Foreign Interference in Canada’s Democratic Processes and Institutions (“**NSICOP Report**”) during *in camera* hearings held in August 2024. 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 the Director of CSIS from 2017 until June 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] **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.

## 2. Examination by Commission Counsel

### 2.1 General Themes and Statements

- [6] [This section contains information provided by the witnesses on various topics discussed throughout the examination. The information was not necessarily provided in the order in which it appears here].

#### 2.1.1 The purpose of intelligence reports

- [7] Mr. Vigneault explained the dual purpose that intelligence reporting can serve: as a source of information for CSIS intelligence officers to analyze, and to provide information for decision-makers outside of the Service that allows them to react accordingly. He emphasized that information management and flow of information is the central question for the Commission; how can intelligence best be used, discussed, and ingested into the machinery of government to allow for decision making. He noted that not every CSIS intelligence report will generate discussion at senior levels, however, he also added that CSIS seeks to broaden the understanding of senior decision-makers and advance common work on issues that may not be fully understood within government. The Service wants to encourage decision makers to come back to the Service, ask questions and then consider how they can take responsibility for the information they receive. He considered that the issue of acting on intelligence, and the

purposes for which it is distributed, is fundamental to intelligence governance within government.

- [8] In response to a question from the Commissioner, Mr. Vigneault added CSIS can flag reports that ought to be brought to the attention of senior officials within each department and that this is often done by way of dissemination lists. He noted that the use of restricted dissemination lists that distribute intelligence only to certain, named recipients was flagged in certain reports as an issue, but considered that this was part of the intelligence governance framework. No one gets access to all the intelligence. For instance, as former Director of the Service, he was not able to read all the intelligence reports produced to understand relevant information; he relies on a team to conduct this work. He said that each agency should have its own specific process to flag and digest intelligence that is relevant for its senior officials.
- [9] Mr. Vigneault noted that intelligence governance is evolving and had changed [in recent years]. The Deputy Minister Committee for Intelligence Response (“**DMCIR**”) is now one of the key means to identify and discuss, in an organized fashion, the intelligence that is relevant to the work of deputy ministers.

### 2.1.2 Reporting under Section 16 of the *CSIS Act*

- [10] Ms. Henderson explained that the “section 16” information referred to the information that Global Affairs Canada (“**GAC**”) tasks CSIS to collect [under s. 16 of the *CSIS Act*, which sets out CSIS’ foreign intelligence assistance mandate].
- [11] Ms. Henderson noted that s.16 reporting has a limited dissemination. She added that, when CSIS collects information under s. 16 of its mandate, it may not report on any Canadian individuals, officials or corporations. As such, CSIS is required to minimize the names of Canadians when it shares s. 16 reporting. If a department considers that the names are required to understand the context of a report, the department can contact CSIS and request the identities be unsuppressed. CSIS tracks and keeps a record of these requests. Ms. Henderson, responding to a question from the Commissioner, added that CSIS decides whether the name(s) will be shared or not.

She noted that this process had led to a recent discussion with the Federal Court, because of an issue where the Communications Security Establishment (“**CSE**”) disclosed Canadian identities in s. 16 reports without consulting CSIS. This led CSIS to work with the Federal Court on setting new parameters to determine how it would engage in the dissemination of s. 16 reporting.

### 2.1.3 “Wittingness”

- [12] Mr. Vigneault identified three broad categories of members of Parliament (“**MPs**”) when assessing their activities [related to potential foreign interference (“**FI**”)]. Clearly, some MPs have no awareness of the FI threat and are surprised when CSIS speaks with them or they read some piece of information. Others know what FI is and that there is a line, but are unsure of its precise boundaries. A smaller subset of elected officials are plainly aware that their actions cross the line into FI.
- [13] The witnesses, including Mr. Vigneault and Ms. Lloyd, highlighted throughout their testimony that the Service’s focus is on the activities of the threat actor [*i.e.*, the foreign state or an individual acting on the state’s behalf] not necessarily the wittingness of an MP. Mr. Vigneault indicated that the heightened interest in the ‘wittingness’ of MPs illustrates the need for individuals who consume intelligence for policy development to come back to CSIS and ask follow up questions when they are concerned about behavior reported in intelligence reports. He noted that until recently, CSIS had not received these types of questions.
- [14] In some cases, CSIS has collected sufficient intelligence to determine that an MP may have, in their own right, and as a result of their ties to another threat actor, been suspected of posing a threat to the national security of Canada. However, this has happened very few times in the Service’s history.

### 2.1.4 Threat reduction measures and awareness of FI

- [15] The witnesses discussed threat reduction measures (“**TRMs**”), including one that involved briefing parliamentarians on FI concerns that may arise from their interactions

with foreign government officials. [One report on the TRM outcomes stated that the TRM exposed a lack of FI awareness among Canadian politicians]. Ms. Henderson stated that she was not surprised by this conclusion and noted that CSIS has tried to raise awareness of the FI threat and general national security threats among MPs and within the wider Canadian population. Mr. Vigneault concurred and stated that this lack of awareness was why CSIS had, starting in 2018, begun speaking more publicly – in CSIS annual reports, in parliamentary committees and in speaking engagements – about the nature of the threats Canada faces.

[16] The witnesses were asked whether this suggested that some of these MPs may have been unaware that they were crossing lines, or not entirely certain where those lines might be. Mr. Basler responded that the focus of the TRM was not the MPs. The TRM was directed at the foreign state and meant to reduce the threat undertaken by that state. The Service was not looking at MPs as having crossed lines, necessarily; that was not the purpose for which an MP was or was not briefed in the TRM. Rather, the Service assessed whether the MP was engaged with a known threat actor. Mr. Basler emphasized that in the majority of cases, the focus is on the threat actor, not the person being impacted by the threat (e.g., the MP). He noted that in some cases, the relationships may have crossed lines, but by no means would all of it be characterized in that manner.

#### 2.1.5 Providing classified information to parliamentarians

[17] The witnesses discussed TRM briefings to Parliamentarians in 2023. CSIS provided classified information to certain MPs under a TRM. Some of these MPs then used Parliamentary privilege to disclose the classified information they had received during the briefing. Mr. Vigneault said that some of the information the MPs disclosed was, at least in part, inaccurate. Mr. Vigneault said that this shows that CSIS has to be mindful when it provides classified information to MPs, because the MP can use parliamentary privilege to disclose it without legal consequences. He said this is a very sensitive area for CSIS.

- [18] Mr. Vigneault explained that, when communicating classified information to parliamentarians, CSIS has to consider its statutory obligations, as well as the Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians (**the “Directive”**). This Directive requires that CSIS take action, including, but not limited to, a TRM, when it becomes aware of a threat. CSIS must consider the nature of the information, its source, and the risks that the source becomes exposed. CSIS also considers other alternatives, to determine whether another type of discussion (such as a defensive briefing), that may not involve classified information, may achieve the desired objective and help the person change their behaviour.
- [19] Mr. Vigneault explained that the other security and intelligence community partners around CSIS can help to identify other options when the risks of using classified information are too significant. He noted that the Government is currently trying to identify the best ways to address this issue.
- [20] Mr. Vigneault testified that, when there is an imminent risk to the life of an individual, CSIS immediately engages police authorities while taking measures to protect the source. Ms. Lloyd noted that CSIS had no information that there was any threat to life or physical harm to parliamentarians and that, if CSIS were to encounter this type of information, it would immediately engage the Royal Canadian Mounted Police (**“RCMP”**) or the relevant police authorities to ensure the physical protection of the person. Ms. Lloyd noted that these communication channels are already established and that CSIS has the ability to engage them quickly.
- [21] Ms. Lloyd added that, if the information does not relate to physical harm, the Governance Protocol for the Directive requires that CSIS contemplate whether or not classified information is to be given to a parliamentarian, depending on whether it can be done within the law, but also in consideration of the need to protect the Service’s investigation methodologies and human sources. There is therefore flexibility in the Protocol.

- [22] Ms. Tessier noted that this evidenced the need to increase general awareness of the intelligence collection process. She believes that, if people have a better understanding of the impacts of revealing classified information on the Service's activities, operations, and intelligence collection, they may react better, or know how to react so as not to expose a source. As she has said in the past, there is an insufficient culture or knowledge of intelligence [in Canada], though the situation is improving. Ms. Tessier stated that it is also important to increase understanding of the limited scope and purpose of intelligence. She further noted that it needs to be understood that CSIS is not always the agency or department responsible for, or best placed, to act on intelligence.
- [23] Mr. Vigneault added that issues can arise either when people are insufficiently informed about intelligence, or when they dismiss intelligence because of preconceived ideas. He indicated that he had observed a lot of public comments that demonstrated a lack of understanding on both these fronts. He considered that the educational work undertaken by the Commission and CSIS to explain both the use and limitations of intelligence is important in that context.

#### 2.1.6 Informing political party leaders about intelligence regarding members of the party

- [24] Mr. Vigneault noted that it is a challenge to identify the authorities, actions, and decisions that a political party leader might use to ensure that their caucus behaves appropriately and to reduce the threat, without disclosing the classified information that they have received.
- [25] Mr. Vigneault said that, in order for intelligence about MPs to become actionable, it would be useful to put in place a system to allow party leaders to receive classified information. The law has just been amended [Bill C-70] so perhaps this will enable the RCMP and others to act. Informing party leaders that a member of their party is taking actions, which CSIS assesses to be national security risks, could allow the party leader to take appropriate measures to prevent that individual from representing the party. Mr.

Vigneault recognized that it was not easy to enable the persons who have this authority to exercise it, but questioned whether the *status quo* was acceptable.

[26] Mr. Vigneault stated that the discussions on how to inform opposition leaders of intelligence have been going on for years. This dynamic [where the intelligence relates to a member of another political party] is why the Service supported NSICOP's recommendation from 2019 that opposition leaders should receive regular classified briefings on national security, including FI. Sometimes, the Prime Minister, as head of the executive, needs to receive information about another party. But there is a tension in the Westminster system since the head of the executive is also the head of a party, meaning they will receive information on other parties. Mr. Vigneault testified that over the past few years he has raised that the government needs to find a way to handle this dynamic and to have the head of the Service give briefings to the leaders of opposition parties. He has asked certain Five Eyes counterparts who work on national security about how they manage these tensions. He said they have done so successfully for several years. He testified that they need to find a way to inform party leaders, since these individuals have the power to appoint people to specific functions within caucus, and having the information would allow them to make decisions about individuals based on national security information.

#### 2.1.7 Protective Security Briefings

[27] Ms. Lloyd explained that a protective security briefing ("**PSB**") is one of the many tools that CSIS can use to engage with individuals. PSBs aim to sensitize an individual to the nature of the threat that they might be facing. They are almost always, at the unclassified level and constitute a generalization of classified information. Mr. Vigneault added that, in most cases, PSBs will discuss the measures that the individual can take to protect themselves.

[28] The person receiving information through a PSB is not legally prohibited from disclosing it. However, in the context of the PSB discussion, which is informed by classified



information, it is implicit that the information should not be disclosed, and it is general practice to advise the recipient that they should not disclose the information.

#### 2.1.8 Vetting for security clearances and Order in Council Appointments

[29] Ms. Lloyd noted that there is an ongoing challenge in CSIS' ability to share classified information. CSIS has engagements with the Government to give advice vis-à-vis Order in Council appointments that involve, in some instances, section 15 investigations or section 13 advice. CSIS might meet with the MP as part of its assessment. In some instances, MPs may have expectations that they are going to be offered certain positions and may want to understand why they are not ultimately chosen for those appointments. CSIS is sometimes asked to consider whether they can share information with the MP. This is a challenge for CSIS, because it may not be possible to provide the MP with information regarding the reasons why they were not appointed without revealing sensitive information.

[30] Mr. Vigneault noted that CSIS does not make decisions regarding appointments; they are consulted. Ms. Lloyd noted that parliamentary secretaries are not necessarily given security clearances.

#### 2.1.9 Delineating FI from personal beliefs

[31] Mr. Vigneault stated that, where an allegation is that an MP is advancing the interests of a foreign state, the situation is complex. The parliamentarian might have their own views on a point that is relevant to the interests of a foreign state. Where parliamentarians have ties to a foreign state, the interests of that state and the personal convictions of the MP might intersect. The actions of the MP become FI when they are undertaken at the request of the foreign state. Delineating the interests of a foreign state and the personal beliefs of an MP involves a particularly challenging and sensitive analysis, especially in the case of MPs with ties to a diaspora community. This nuanced analysis forms part of CSIS' ongoing efforts to provide increasingly sophisticated assessments of the activities of MPs.

[32] Mr. Vigneault noted that, to navigate these nuances, the definition of FI (as being clandestine, deceptive, coercive) is key, as it allows for the distinction between what may be lawful support for the activities of a foreign state, versus covert support.

#### 2.1.10 Declared vs. undeclared intelligence officers

[33] Ms. Henderson explained that a “declared” intelligence officer is a member of a foreign state’s diplomatic mission in Canada. These individuals declare (to Canadian authorities) their status as a representative of the intelligence service of the foreign state. This is common practice.

[34] Declared intelligence officers engage with intelligence partners in Canada, for example on security matters of joint interest or importance. Declared intelligence officers also maintain relationships with declared intelligence officers from other countries with diplomatic missions in Canada. These individuals are declared to the host country, not to the public.

[35] An “undeclared” intelligence officer, on the other hand, has not declared their status as a representative of the intelligence service of a foreign state but is engaged in undeclared intelligence work within Canada under another title in the diplomatic community. This is colloquially known as a “spy”.

#### 2.1.11 Factual review of NSICOP Report

[36] The witnesses discussed the factual review that CSIS and other departments/agencies perform after a review body prepares a report. Mr. Basler explained that it is a very fine line, because the department/agency cannot influence the review body’s analysis or conclusions. The agency might note when the review body has relied on the wrong document or if there is something fundamentally incorrect. The review agency will most often make a correction or come back for details or precision.

[37] CSIS stays away from commenting on conclusions, analysis or wording. Once CSIS has pointed out an error, it is up to the review body to decide whether to correct the error or not.

## 2.2 Specific Allegations

[38] [This section contains information provided during the examination on specific allegations in the NSICOP Report regarding possible witting or semi-witting involvement of parliamentarians in foreign interference activities. Some of these allegations involved former parliamentarians, while others involved current parliamentarians. Some of these examples appear on the list of significant instances of FI. Mr. Basler explained why this was. Mr. Basler reiterated that what made it on the list went through discussions with other agencies at the senior level (GAC, CSE, PS, and PCO). All agencies looked at the same information as CSIS and agreed on the assessment of that intelligence to make sure the list was solid from all perspectives. All except one of the incidents referred to in the Unclassified CSIS IR and CAN.SUM.000031 [the Suspected Instances Topical Summary] were referred to in the NSICOP report.]

### 2.2.1 NSICOP Report Allegation 1 of an elected official wittingly assisting foreign state actors

[39] Commission counsel referred the witnesses to an allegation identified in the classified version of the NSICOP Report, the public version of which reads:

Some elected officials, however, began wittingly assisting foreign state actors soon after their election. [\*\*\* Three sentences were deleted to remove injurious or privileged information. The sentences described examples of members of Parliament who worked to influence their colleagues on India's behalf and proactively provided confidential information to Indian officials. \*\*\*].<sup>1</sup>

[40] Commission counsel also referred the witnesses to underlying CSIS reporting relevant to Allegation 1 of the paragraph of the NSICOP Report quoted above.

[41] Ms. Henderson noted that the dissemination of the underlying reporting was limited.

[42] Commission counsel asked the witnesses about the Service's assessment of the wittingness of the MP involved in Allegation 1. Ms. Lloyd explained that the information CSIS has about MPs is largely collected incidentally. The process for assessing

---

<sup>1</sup> Para. 55.

individuals who engage with threat actors is time- and point-specific. Ms. Lloyd emphasized that, when CSIS collects information on threat actors, it does not necessarily assess individuals engaging with the threat actors, unless it is part of a determination of investigative steps and so CSIS would not necessarily have made an assessment of the MP's wittingness.

[43] Mr. Vigneault commented that one of the challenges for the Commission is to see and track the evolution of the FI threat over time. Indeed, NSICOP has noted that while CSIS has produced a significant amount of intelligence about FI over the past years, the response to that intelligence was not necessarily there. Early on, CSIS treaded very carefully in its investigations around elected officials. Mr. Vigneault noted that since 2018 or 2019 there had been an evolution around the FI threat that had broken new ground. There was a turning point where other government departments and agencies recognized the need to react to and address the threat differently. The panel highlighted that CSIS has been undertaking FI investigations against democratic institutions since the late 1990s.

[44] Mr. Vigneault indicated that, in addition to this evolution within other government departments, CSIS had also evolved internally in its understanding of the work it can do with respect to elected officials, despite the sensitivities that arise in related investigations. He noted that there had been a full reversal with respect to intelligence concerning elected officials; while CSIS had at first perceived some discomfort, government officials now seek more of this information in order to address potential threats. Mr. Vigneault indicated that determining whether a parliamentarian is doing the bidding of a foreign state remains challenging, because the Service's investigations are focused on the foreign state threat actors, not necessarily the parliamentarians. Mr. Vigneault's view was that the Commission will need to grapple with the important question of establishing an accepted norm [for the actions of parliamentarians]. One that takes into account all checks and balances of a democracy, including the right to privacy of elected officials. This question is key to addressing the foreign interference threat.

- [45] Ms. Lloyd added that CSIS has taken steps in relation to Allegation 1 after the publication of the NSICOP Report. Ms. Lloyd underscored that the Service's focus in situations such as Allegation 1 in the NSICOP report has to be on the foreign actors' activities, as opposed to Canadians conducting interference, in some way, in democracy. It is all directed by the threat actor.
- [46] Ms. Henderson added that it is a sliding scale in terms of whether a person may be compromised, and CSIS' assessment moves up and down along that scale over time as it collects more intelligence. One day it might really seem that an individual is compromised, but the next day you might get another piece of information that changes that.
- [47] Ms. Lloyd noted that CSIS is not in a position to know how NSICOP came to its conclusions. Mr. Basler added that NSICOP had chosen the wording of the NSICOP Report, not CSIS. It may, in some respects, reflect the wording of the documents of the Service, but not always in the same context. He noted that NSICOP was also a committee of parliamentarians, which had assessed the activities of parliamentarians through the eyes of parliamentarians, based on intelligence reporting of foreign states engaging with parliamentarians. From this posture, the members of NSICOP may have been passing judgment on the activities of their colleagues in the House of Commons whose behaviour they considered to have crossed the line.
- [48] Mr. Basler noted that CSIS agrees with some aspects of the NSICOP Report. He added that NSICOP assessed the activities of parliamentarians with their own experiences and knowledge of what is appropriate as members of the House of Commons. Mr. Basler noted that, in some cases, CSIS may have reported or assessed that an MP is witting, but Mr. Basler did not have a specific recollection of whether CSIS had used that term in relation to the MP involved in Allegation 1 cited by NSICOP as a witting politician.
- [49] Mr. Basler acknowledged that this MP's activities were not included as one of the seven significant instances of FI identified in the CSIS Stage 2 Institutional Report (**"CSIS IR"**). He did not believe that this allegation was on the initial list of incidents [in his

previous *in camera* testimony, 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]. Mr. Basler explained why, in his view, this incident may not have met the criteria the government applied when identifying significant instances.

### 2.2.2 NSICOP Report Allegation 2 of an elected official wittingly assisting foreign state actors

[50] Commission counsel referred the witnesses to another allegation identified in the classified version of the following paragraph of the NSICOP Report:

Some elected officials, however, began wittingly assisting foreign state actors soon after their election. [\*\*\* Three sentences were deleted to remove injurious or privileged information. The sentences described examples of members of Parliament who worked to influence their colleagues on India's behalf and proactively provided confidential information to Indian officials. \*\*\*].

[51] [The NSICOP Report states that the MP referred to in Allegation 2 is the same MP as in Allegation 1. However, the intelligence reporting cited in the footnote for Allegation 2 is about a different MP. Commission counsel asked the witnesses if they were able to explain this discrepancy between the allegation in the NSICOP Report and the intelligence reporting]. Mr. Basler began by noting that NSICOP did not identify the MPs that it referenced in any given paragraph, so CSIS did not know who, on a first read, was being referenced in any of the allegations or assertions. CSIS attempted to reverse engineer the NSICOP Report to identify which MPs the Report was referring to.

[52] CSIS believed that, by reverse-engineering the NSICOP Report, it had identified the MP involved in Allegation 2. Mr. Basler testified that this threat was no longer a concern and acknowledged that there is an ambiguity because the document that is listed in the footnote of the NSICOP Report refers to a certain MP, while the paragraph of the classified NSICOP Report appears to identify another MP.

- [53] Commission counsel referred the witnesses to underlying CSIS reporting to which Allegation 2 likely refers.
- [54] Mr. Basler indicated that NSICOP's methodology is to review disseminated intelligence products and make follow-up inquiries. Mr. Vigneault noted that the disseminated reports were much less detailed than the underlying intelligence to which the Commission had access.
- [55] Mr. Basler indicated that Allegation 2 is listed in the CSIS IR and is viewed by the Government as a significant instance of FI.
- [56] Commission counsel asked what the Service's assessment was, if any, of the MP's knowing participation in foreign interference activities. Mr. Basler indicated that he believed that the MP had heightened awareness of what FI activities are. Mr. Basler testified that this threat is no longer a concern.
- [57] Mr. Vigneault was not aware of any other actions taken by CSIS or other government departments in response. He noted that he had less visibility over the actions of other government departments. Mr. Basler noted that the threat is no longer a concern.

### 2.2.3 NSICOP Report Allegation 3 of an elected official wittingly assisting foreign state actors

- [58] [Commission counsel referred the witnesses to underlying intelligence reporting related to the allegation at paragraph 55 of the NSICOP Report that an elected official proactively provided confidential information to Indian officials. An intelligence report suggests that the MP allegedly provided confidential information to an Indian official. However, at the time the MP is alleged to have done this, the information had already been made public.]
- [59] Commission counsel referred the witnesses to another piece of underlying intelligence reporting related to the allegations in paragraph 55 and the alleged sharing of confidential information. Mr. Basler noted a concern about the MP's actions, but acknowledged that CSIS did not know the MP's intentions.

- [60] Commission counsel referred the witnesses to the 2022-2023 Annual s. 6(4) Report to the Minister on CSIS Operational Activities. Mr. Vigneault explained that the *CSIS Act* requires that, each year, the CSIS Director submit a classified report to the Minister about the Service's activities. This is a non-exhaustive report of its operational activities so that the Minister is aware at a high level of the Service's activities. These reports are also reviewed by the National Security Review and Intelligence Agency to see if there are any errors or omissions, to ensure the accountability of CSIS.
- [61] Commission counsel referred the witnesses to an excerpt of the Annual Report relating to the allegation in Allegation 3 and referring to the information shared by the MP as having been confidential. [The Annual Report does not name the MP, but reports the events].
- [62] Commission counsel asked the witnesses to agree that, based on the information before the Commission, the information was no longer confidential when the MP shared it. Mr. Vigneault hesitated because he thought he recalled some intelligence was dated earlier than what was before the Commission. The witnesses undertook to verify if such information existed, and if so, to produce it. [Subsequent to the hearing, the Commission was advised that the Service had no indication that confidential information was shared by the MP].
- [63] Commission counsel referred the witnesses to the language of the NSICOP Report, which is more specific than the language in the CSIS Annual Report, and asked the witnesses to agree that, based on the information before the Commission, the statement in the NSICOP Report is inaccurate.
- [64] Ms. Lloyd added that is important to recognize that CSIS's information is limited. Neither the MP nor the other individual referenced in the intelligence are subjects of investigation. According to Ms. Lloyd, what is of concern here with respect to foreign interference is the relationship between the MP and the threat actors, and the engagement that suggests the MP is taking, or purporting to take, activities on behalf of the foreign threat actor. This raises concerns as to the foreign state actor's ability to



have their national interests met above Canadian interests through that MP. [Further to the undertaking agreed to during the examination, CSIS has no information that the MP provided confidential information to Indian officials. CSIS information merely implied that some information (not necessarily confidential information) would be shared discreetly.]

- [65] Commission counsel noted that Allegation 3 did not make it into the CSIS IR as a significant instance of foreign interference. Mr. Basler explained that this was, in part, due to some of the limitations regarding the intelligence on this allegation.
- [66] Commission counsel asked the witnesses about the language of paragraph 55 in the public version of the NSICOP Report and asked whether in the Service's view it is borne out in relation to the MP in Allegation 3. Mr. Vigneault said that it was important to recognize that CSIS is limited in its ability to interpret NSICOP's words. The witnesses confirmed that the summary at paragraph 55 of the NSICOP public report is a summary of NSCIOP's conclusions, not the Service's conclusions. Further, Mr. Basler noted that the language of the summary in the Public NSICOP Report went through national security confidentiality review, which removes any information that might cause injury to the national interest. He underlined that this is not an accuracy review, it is a review for injury. Mr. Basler noted that it is important to recognize that nuance is often lost in the process of national security confidentiality review.

#### 2.2.4 Allegation of a “textbook example” of FI

- [67] The Commission examined an allegation at paragraph 56 of the NSICOP Report that was described as a “textbook example of foreign interference that saw a foreign state support a witting politician”.<sup>2</sup> The witnesses confirmed that the description of the politician as “witting” is NSICOP's conclusion, not the Service's. Commission counsel referred to an intelligence product related to this allegation. Mr. Basler confirmed that this product describes this incident as a “textbook example of foreign interference”, but does not describe the MP as a “witting politician”. Commission counsel took the

---

<sup>2</sup> Paragraph 56 of the Public NSICOP Report.

witnesses to a written response to questions posed by the Commission prior to the examination (CSIS “**Written Response**”) regarding this allegation, which states that “the extent to which [the MP] is aware of the details [...] or that they constitute foreign interference remains an intelligence gap.” Mr. Basler confirmed that this was a fair statement.

#### 2.2.5 Allegation regarding interactions with a foreign intelligence officer

[68] The Commission explored an allegation in the NSICOP Report in which a person was described as an undeclared intelligence officer but was in fact [as confirmed in CSIS intelligence products and its Written Response] a declared intelligence officer. Mr. Basler indicated that NSICOP’s statement could be somewhat factual in that the individual was declared to the Government of Canada. Some MPs, likely this MP, were aware of his status as a declared intelligence officer, while other MPs and the public were not.

[69] Mr. Vigneault said that an MP knowingly interacting with an intelligence officer from a foreign country is cause for concern as is an MP interacting with an undeclared intelligence officer presenting as a diplomat.

#### 2.2.6 Allegation regarding an MP proactively providing an intelligence officer with information received in confidence

[70] The Commission explored the allegation at page 26 of the NSICOP Report whereby an MP is alleged to have passed on information that was provided to them in confidence to a foreign intelligence officer. In the CSIS Written Response, the Service acknowledged that “[i]t is not known whether the MP had been advised that they were to keep that information in confidence.”

[71] Commission counsel referred the witnesses to underlying intelligence indicating that the information that had been provided to the MP was unclassified.

[72] Mr. Vigneault confirmed that the information in this case was not classified, by definition, but that based on the context and purpose for providing the information, MPs would

have understood that the expectation was that they maintain discretion. The witnesses could not recall whether this was explicitly stated to the individuals when they received the information.

- [73] Mr. Basler noted that classifications of information have definitions – Unclassified means no harm to the national interest, Secret means grave harm and Top Secret is exceptionally grave harm. This does not mean that unclassified information is not still sensitive; for example, CSIS may give information in a briefing that it does not want to be shared with the media or more broadly.
- [74] The NSICOP Report refers to the information as “privileged”. Commission counsel asked the witnesses whether they were aware of what privilege applied to this information. Mr. Basler indicated that the information was privileged in the sense that it was provided to specific individuals. However, he agreed that it was not protected and was unclassified. Mr. Vigneault indicated that the information was not “privileged” in the formal sense that there was a prohibition on disclosing it. According to Mr. Vigneault, however, the context of the briefing made it very sensitive information and would have given rise to an expectation that the information would not be disclosed to a third party.
- [75] For an MP to give this information to a foreign intelligence officer raises a red flag. Mr. Basler added that this is indicative of a concerning relationship.
- [76] In the context of this discussion, Ms. Henderson added that we are very tied up with the definition of classified information, which overlooks the fact that the unclassified information was provided by a Service expert whose knowledge base comes from a pool of classified information. It would behoove the individuals receiving the information to recognize that in the context of geopolitics they should maintain the privilege of the briefing rather than divulge its contents to a foreign intelligence officer.
- [77] Commission counsel referred the witnesses back to intelligence reporting to discuss the information that was allegedly disclosed to the intelligence officer. Ms. Henderson agreed that it was not necessarily the information provided to the intelligence officer that was concerning but the very fact that this conversation was happening.

- [78] Mr. Basler acknowledged that this incident was not identified as a significant instance of FI in the CSIS IR.
- [79] The Service witnesses agreed that, in respect of this allegation, NSICOP used stronger language than the Service used.
- [80] Commission counsel referred the witnesses to other information in CSIS holdings about the nature of the relationship between the then-member of Parliament and the intelligence officer. Ms. Lloyd noted that MPs may have a variety of legitimate reasons for being in contact with representatives of a foreign government. The contact with a foreign official can be established through any variety of reasons but it is what the MP does with the connection and how they comport themselves that is relevant.

#### 2.2.7 Allegation – concerns with an MP being compromised by a foreign state

- [81] [Commission counsel referred the witnesses to an allegation contained in the classified NSICOP report indicating that an MP had been compromised using specific inculpatory language. Commission counsel queried whether NSICOP's characterization was directed at the correct MP, and whether the correct country had been identified in the allegation. The Service witnesses responded that reporting refers to a different country than that which NSICOP identified.]
- [82] The Service witnesses noted that this was a difficult allegation for the Service to reverse-engineer. Certain intelligence used the specific inculpatory language, but in relation to the MP's relationship with a different country. However, Mr. Basler added that the MP's relationship with both foreign states was concerning.
- [83] They further noted that NSICOP incorrectly ascribed the inculpatory language as an assessment of the Service. In fact, it was not the Service's assessment, but language used by a third party in an intelligence report viewed by NSICOP.

#### 2.2.8 Allegation concerning covert support from Pakistan

- [84] The witnesses previously testified about this instance of suspected FI during their *in camera* examination on July 10, 2024.

- [85] Mr. Basler confirmed CSIS understands that Pakistan worked to support a preferred candidate's election.
- [86] Mr. Basler testified that this information was shared with both Elections Canada ("**EC**") and the Office of the Commissioner of Canada Elections ("**OCCE**"). The Service shared this intelligence with them through the construct of the SITE TF. The Service presented an overview of threats to elections that could overlap with their mandate or interest, and provided them with reading packages on this. The reporting on this MP was provided in the course of these reading sessions. Commission counsel asked whether this information was shared with EC and OCCE because it indicated a potential violation of the *Elections Act*. Mr. Basler said that this could have been the case, or it could have been presented as contextual information to improve understanding of threats to the election. Even if not directly related to EC or the OCCE's mandates, it may have helped them understand the methodology of certain state actors.
- [87] Mr. Vigneault testified that the CSIS' work in terms of collecting and sharing intelligence has evolved over the years. He explained that, while the Service can take action by using its TRM authority, it is generally someone else's responsibility to take action. In this context, the Service has worked with the Office of the Commissioner of Canada Elections to develop a Memorandum of Understanding. The intention was to figure out a way to work together since the Service has the information and EC has the mandate. This relationship continues to evolve. The Service's intention was to ensure the OCCE could use Service intelligence to have an impact and make Canadians safer. This is why these meetings and protocols were developed. The Service is finding different ways to make its intelligence more useful.

#### 2.2.9 Allegation concerning the transfer of funds from the Government of India ("**GoI**") to an MP

- [88] Commission counsel referred the witnesses to paragraph 68 of the NSICOP Report and to reporting that appeared to be related to this allegation. The reporting states that the

Indian proxy believed that an MP that received financial support had agreed to support Gol positions.

- [89] Commission counsel referred the witnesses to a sentence in paragraph 68 of the NSICOP Report, which states: “CSIS did not share this information with the RCMP or with the Commission of Canada Elections.” Mr. Vigneault could not recall any specific discussion but noted that the intelligence was limited. As such, while he does not know why this specific information was not shared, he is not uncomfortable that it was not, under the circumstances.
- [90] Ms. Lloyd added that the reporting shows the intent of the threat actor but not the impact on the MP. Ms. Lloyd testified that this proxy was well known to the Service and that the Service believes they either did or attempted to do the things described in the reporting.
- [91] This MP had received a briefing under a CSIS TRM.
- [92] Ms. Lloyd confirmed that the intelligence reflects the proxy is under the impression the MP is someone upon whom they can rely.

#### 2.2.10 Allegation concerning Indian interference in the CPC Leadership Race

- [93] Commission counsel referred the witnesses to paragraph 73 of the NSICOP Report, which states that India allegedly took steps to interfere in the CPC leadership race.
- [94] The witnesses previously testified about this allegation during the *in camera* hearing on July 10, 2024.
- [95] Commission counsel referred the witnesses to documents outlining some of the actions the Gol may have taken in this regard. Mr. Basler noted the documents do not suggest the candidate would have been aware of the alleged support.
- [96] Ms. Lloyd testified that this allegation was referenced in a classified briefing she gave to the CPC leader’s Chief of Staff in June 2024.

- [97] Ms. Lloyd confirmed that the Chief of Staff had received a Top Secret level clearance before receiving this briefing. She noted that this briefing fit within the broader issue discussed by Mr. Vigneault of providing classified information to party leaders to increase their resilience with respect to foreign interference. She noted that this conversation around the appropriate protocols and ways of organizing this communication of information was ongoing within government, including at DMCIR.
- [98] Ms. Lloyd noted that the Leader of Opposition had, to date, declined to receive a security clearance, which is why CSIS delivered the briefing to his chief of staff. The briefing in this case was with regard to potential GoI interference. Further to discussion of the issue at DMCIR, the government believed that this information needed to be presented to the Conservative Party.
- [99] Ms. Lloyd explained that she and the Deputy National Security and Intelligence Advisor to the Prime Minister, Dan Rogers, provided this briefing, which was arranged by PCO. The briefing contained information that is reflected in the NSICOP Report, as well as other information that the government considered necessary to provide to the party.
- [100] Ms. Lloyd noted that the objective of sharing the classified information was to build the resiliency of the CPC in relation to this potential avenue of FI by threat actors. The objective of the briefing was to raise awareness within the party about the areas that it should be monitoring and the actions that it could take within its purview. [For instance, in sharing certain information about the tactics used by foreign states, the party could better identify possible instances of FI and be more critical about behaviour that might otherwise have been regarded as normal.]

### 3. Examination by the AGC

- [101] With respect to the allegation discussed in section 2.2.7, the AGC referred the witnesses to CSIS reporting about India's FI activities. Mr. Basler said that there may have been confusion in attribution on the part of NSICOP because some MPs may have a beneficial relationship with several foreign governments.

[102]The witnesses were asked for their perspectives on the NSICOP Report.

[103]Mr. Vigneault stated that he accords a lot of significance to the NSICOP Report for a number of reasons. NSICOP is composed of parliamentarians. Given that CSIS has been accused of not adequately understanding the political process, having the perspective of political actors who are reviewing CSIS intelligence is important.

[104]Mr. Basler, having worked with NSICOP on the public version of the report, noted the strong interest that NSICOP had in disclosing as much information as possible, and in the process its public report disclosed important information that the Service would not have had the authority to disclose on its own.

[105]Mr. Basler added that he sees the NSICOP Report as a ground-breaking report with reference to FI. In his view it is generally accurate. Mr. Basler stated that the big picture in outlining the nature of the threat and the efforts undertaken by foreign states to influence parliamentarians is largely accurate; the details or wording may be stronger than what CSIS would have chosen, but [NSICOP] is looking at things through a different lens. He finds it a groundbreaking effort on their part to try and detail these threats in a manner that is open and public and can be understood by other members of Parliament.

[106]Ms. Lloyd noted that the NSICOP Report helps to amplify the seriousness of the threat. MPs have recognized that there is a need to have a public dialogue about both the threat actors' activities and what responses are possible.

[107]Ms. Henderson added that NSICOP provides the Service with an opportunity to present information to all parties, not just the Government and its executive.

[108]Mr. Henderson noted that CSIS has been struggling with transparency and trying to become more transparent. NSICOP coming forward with its public report got the message out more broadly.

[109]Ms. Tessier said that she was pleasantly surprised by the amount of information contained in the public report. She thinks it is important to have this conversation. She



recalled being asked by the media whether she was “surprised” by the information contained in the public report and answered that she was not “surprised” because the Service has been looking at these issues for quite some time. She notes that the nuances that are being raised by the Commission are important. That said, the nature of these activities and the fact that they are happening in Canada is important to highlight. There is not enough discussion about this in Canada; in fact there is astoundingly little understanding of national security issues in Canada.

[110]Mr. Vigneault noted that NSICOP has enabled more details about FI events to be made public, in addition to those disclosed in the CSIS Annual Report and the Commission’s first public report. In the context of foreign interference, these reports have allowed more information to be made public. This has changed the dynamic: there is more specific information in the public sphere.