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

Interview Summary: David Vigneault, Michelle Tessier, Cherie Henderson

Senior officials from the **Canadian Security Intelligence Service ("CSIS"** or **"the Service")** were interviewed in a panel format by Commission counsel on February 13, 2024. The interview was held in a secure environment and included references to classified information. This is the public version of the classified interview summary that was entered into evidence in the course of the Commission's in camera hearings held in February and March 2024.

Notes to Reader:

- Commission Counsel have provided explanatory notes in square brackets to assist the reader.
- This summary has been prepared pursuant to subclause (a)(iii)(C)(II) of the Commission's Terms of Reference. It discloses the evidence pertinent to clauses (a)(i)(A) and (B) of the Commission's Terms of Reference that, in the opinion of the Commissioner, would not be injurious to the critical interests of Canada or its allies, national defence or national security.
- This summary contains information that relates to the Commission's mandate under clauses (a)(i)(A) and (B) of its Terms of Reference. Information provided during the interview that relates to other aspects of the Commission's Terms of Reference has been omitted from this summary, but may be adduced by the Commission at a later stage of its proceedings.
- This summary should be read in conjunction with the CSIS Institutional Report prepared by the Government of Canada and the public summary of the *in camera* examination of CSIS witnesses.

Background

CSIS is Canada's national civilian intelligence service. Pursuant to section 12 of the *CSIS Act*, its core mandate is to "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, [...] report to and advise the Government of Canada."

David Vigneault is the Director of CSIS and has been since 2017. In this capacity, Mr. Vigneault oversees all CSIS activities and engages with domestic and foreign partners.

Michelle Tessier was appointed **Deputy Director of Operations** ("**DDO**") of CSIS in December 2018. She served in this role until March 2023, when she retired from the Service. She had overall responsibility for CSIS operations and would replace the Director as required. In the spring of 2019, following an internal reorganization, she also assumed charge of CSIS's Intelligence Assessment Branch (IAB) through the creation of the Assistant Director, Requirements ("ADR") position.

Cherie Henderson served as Director General of the IAB from 2019 to 2022. In this role, she oversaw the production and dissemination of intelligence reports. In 2021, she took on the position of Acting ADR, formally assuming the role in 2022. The ADR leads CSIS's headquarters operations and analysis sections (IAB). IAB's mandate is to provide timely and relevant intelligence which meets the Government of Canada's stated requirements and priorities.

* * *

Background and Mandate

Intelligence Priorities and Requirements

Mr. Vigneault explained that the process to determine Canada's intelligence priorities is coordinated by the **Privy Council Office ("PCO")**. PCO seeks input from the entire Canadian security and intelligence community and other federal departments concerning their intelligence needs. This includes CSIS, which is one of the main players in helping

to develop the key issues and priorities. The priorities established as a result of this process are then presented to Cabinet, which reviews the suggested priorities and settles on a final list. The final list of priorities includes substantial detail as to the implementation of these priorities. Based on this list, each relevant minister (in CSIS's case, the Minister of Public Safety and Emergency Preparedness) then issues a Ministerial Directive to the applicable agencies.

All witnesses emphasized that this is a collaborative process that ensures that agencies are in a position to operationalize the intelligence priorities. Ms. Henderson noted that the ADM Intelligence Priority Committee, chaired by PCO, held regular meetings to ensure that the security and intelligence ("S&I") collection was meeting government requirements. CSIS also attempts to obtain feedback from clients [the government departments, agencies, and offices that receive CSIS intelligence] to determine if requirements are being met. Ms. Tessier added that CSIS developed intelligence "requirements" based on the intelligence priorities and these requirements allow its various branches and regional offices to effectively operationalize the priorities. These requirements also take CSIS's own capabilities into account.

Mr. Vigneault also noted that some other jurisdictions are very clear and specific with respect to the resources to be allocated to each intelligence priority. In Canada, by contrast, CSIS gets general and informal feedback from clients, from which it attempts to align its resource allocation to meet their intelligence needs.

Feedback on CSIS Intelligence

Ms. Henderson indicated that the feedback received from clients plays a key role in CSIS's efforts to provide relevant intelligence. Ms. Tessier agreed and noted it was challenging to obtain feedback from clients. In this respect, Mr. Vigneault drew attention to the distinction between (i) actionable and (ii) "building block" intelligence. The former calls for government consideration of possible courses of action. The latter helps build a narrative to provide background information regarding an actor or threat more generally. Ms. Tessier indicated that she was aware of government having acted on the basis of certain intelligence products, most saliently with respect to security screening. CSIS

Intelligence Reports ("CIRs"), for example, are usually building block intelligence reports and help a user of intelligence build a bigger picture.

Interaction of CSIS's mandates under ss. 12 and 16 of the *CSIS Act*

All witnesses agreed that, CSIS's s. 16 mandate [s. 16 of the *CSIS Act* mandates CSIS to collect foreign intelligence at the personal request in writing of the Minister of Foreign Affairs or the Minister of National Defence and with the personal consent in writing of the Minister of Public Safety] is broader in scope than s. 12, as it allows CSIS to collect intelligence that relates to a foreign state. Section 16 requests are discussed at the ADM Intelligence Review Committee, chaired by PCO.

Ms. Tessier noted that while the s. 16 mandate is triggered by a request from the Minister of Foreign Affairs, CSIS retains control over the investigative techniques employed. She further noted that information collected by CSIS under its s. 16 mandate can be relevant to its mandate under s. 12, and can be used in s. 12 investigations [under s. 12 of the *CSIS Act*, CSIS shall "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, (…) report to and advise the Government of Canada."]. Ms. Tessier explained that the names of Canadian citizens are generally suppressed in s. 16 reporting. Ms. Henderson added that, with the exception of Global Affairs Canada ("GAC"), clients would not notice any difference between intelligence collected pursuant to CSIS's mandates under s. 12 and s. 16.

Operational Structure

The witnesses were asked to comment on Appendix C of CSIS's Institutional Report [Appendix C, which is classified, is an *Organisational Chart* of the CSIS departments relevant to foreign interference (**"FI"**)]. Mr. Vigneault explained that each position or branch identified in the chart implements the intelligence priorities at various stages of the "intelligence cycle" [government requirements → priorities → planning → collection → analysis → dissemination → feedback]. These directorates all act under the operational authority of the DDO.

As noted above, Ms. Tessier explained that the IAB was formerly detached from the Operations Branch [which was headed by the DDO] but that assessment and operations were integrated in 2019. Ms. Henderson explained that this allowed the assessment branch to cooperate closely with the collection branch in order to identify and remedy intelligence gaps. Mr. Vigneault added that the goal of this restructuring was to foster greater collaboration and coordination between the collection and assessment activities of CSIS, to ensure that the intelligence products that it provides to government agencies and officials are relevant to their decision-making. He noted that a similar objective, in the specific case of FI, led to the creation of the Executive Lead and Foreign Interference Coordinator in 2023.

ADR Directorate

Mr. Vigneault identified the restructuring within the ADR Directorate as another example of this integrated approach. A branch was created within the ADR Directorate to integrate operations and analysis related to FI issues.

Ms. Henderson added that there are also employees in regional offices who are responsible for various phases of the intelligence cycle related to PRC threats. Ms. Tessier noted that all regional offices focus on PRC threats to some extent, but identified the regions which are the most involved.

When asked to comment on an email exchange between a CSIS regional office and an employee of the ADR Directorate who express differing views regarding the assessment of pieces of intelligence, Ms. Henderson and Ms. Tessier testified that this is not unusual: there has always been a healthy tension between regions and Headquarters **("HQ")**, and such discussions and debates between regional analysts and employees of CSIS HQ are frequent and expected. HQ has a broader perspective, looking at everything in context of the information it receives from other sections of CSIS as well as national and international partner agencies. HQ sets the requirements and controls dissemination. With its broader, more strategic perspective it is mindful of overall resource allocation. CSIS regional offices, for their part, are focused on their specific remits, and have in-depth knowledge of the threats and incidents that are occurring in their geographical area.

According to the witnesses, both perspectives bring value to CSIS's activities, and robust discussions enable them to learn from one another and to improve.

Ms. Henderson and Ms. Tessier noted that the exchange reflected in the emails could also be reflective of a concern voiced by the regional offices that they had not been involved soon enough after the new branch in the ADR Directorate was stood up. CSIS implemented the new model incrementally, as it was not certain whether the structure would be successful. In the end it was successful, and personnel from the regional offices now work more closely with the ADR Directorate. According to the witnesses, this has improved the understanding of the headquarters and regional personnel as to their various contributions to the process, and thus the effectiveness of intelligence collection, analysis and reporting.

Information Flow

CSIS's Intelligence Products

In addition to the intelligence products that were included in Appendix E to the CSIS Institutional Report [a description of eleven intelligence products produced by CSIS and distributed to other agencies or departments], the witnesses were asked to comment on certain specific types of intelligence products.

In addition to these specific intelligence products, Ms. Henderson discussed the purpose of another specific product. She explained that it was designed to alert people within government who may or may not be aware that they are subject to a threat, or to explain a national security threat to a greater audience that could be impacted. Mr. Vigneault explained that, save for very rare cases, these products were not shared publicly.

Dissemination of CSIS Intelligence – Generally

Ms. Henderson indicated that CSIS disseminates its intelligence products in line with the intelligence requirements and based on the feedback received from, and needs identified by, client departments and agencies. This collaboration is necessary for CSIS to have a constant awareness of a given department's needs and interests so that it can provide useful information.

Ms. Henderson described the process to authorize dissemination of certain intelligence products. Ultimately, the dissemination was always approved by the relevant desk head. She added that, for some particularly sensitive products, dissemination may require a higher level of approval.

Ms. Henderson further explained that, until the fall of 2023, CSIS intelligence products were sent to clients via the **Canadian Top Secret Network ("CTSN")**. Following the leak of CSIS documents to the media, CSIS modified its practices and now uses another channel to transmit information This new mechanism for dissemination allows CSIS to control and monitor access to its intelligence in a secure fashion and to keep track of who accessed reports.

Mr. Vigneault also explained that CSIS combined its use of electronic means with the services of **Client Relation Officers ("CROs")** to provide intelligence to ministers personally [CROs are employees of CSE housed within other departments or agencies and are responsible for providing information to ministerial offices]. If a CRO cannot reach a minister (which happens frequently if the minister is outside the Capital region), the relevant CSIS regional office may host a minister in its office to provide them with intelligence, or in some cases attend at the location of the minister and wait while the document is read.

It was also mentioned that CSIS recently assigned a CSIS CRO to the Department of Public Safety. This helps ensure that CSIS intelligence is brought to the attention of senior officials within the Department of Public Safety and to the attention of other departments or agencies in deputy minister committees or assistant deputy minister committees. This individual is able to provide context to the intelligence as required.

Dissemination of CSIS Intelligence – To Specific Agencies

The witnesses were asked to provide specific information regarding the exchange of intelligence with the following partners:

a. The Royal Canadian Mounted Police ("RCMP")

Ms. Tessier explained that cooperation with the RCMP is, from a formal standpoint, governed by the *OneVision* framework. With respect to FI, cooperation is sometimes

more informal because FI activities are rarely subject to a clear prohibition under the *Criminal Code*. She noted that, during the elections, cooperation with the RCMP specific to FI was reinforced by the Security and Intelligence Threats to the Elections Task Force **("SITE TF")**, of which the RCMP is a member. Ms. Henderson and Mr. Vigneault both emphasized that CSIS has a good relationship with the RCMP. They noted that CSIS sat on many committees of which the RCMP is also a member.

b. The Office of the Commissioner of Canada Elections ("OCCE")

Mr. Vigneault indicated that cooperation between CSIS and the OCCE used to be informal but that the relationship between the two agencies had strengthened in recent years. Exchange of information between the two is governed by a September 2019 memorandum of understanding. Ms. Tessier and Mr. Vigneault both noted that the OCCE's lack of security-cleared employees and facilities created challenges in this respect. To alleviate these challenges, briefings to appropriately cleared employees of the OCCE would typically be delivered in CSIS offices.

c. The Financial Transactions and Report and Analysis Centre ("FINTRAC")

Further to an undertaking, CSIS provided the following information with respect to its cooperation with FINTRAC: FINTRAC discloses certain information that may be relevant to CSIS's mandate. With respect to the 43rd and 44th General Elections, FINTRAC provided information that supported CSIS investigations into two individuals, both of whom became warranted subjects of investigation for their involvement in foreign influenced activities.

d. PCO

All witnesses agreed that CSIS met with PCO staff frequently. Ms. Tessier explained that CSIS would distribute various intelligence products to PCO and would also sometimes respond to specific requests. All witnesses identified the following secretariats as the main ones with which CSIS interacted: the **Intelligence Assessment Secretariat ("IAS")**, the **Security and Intelligence Secretariat ("PCO SI")**, the **Democratic Institutions Secretariat ("PCO DI"),** and the **Foreign and Defence Policy Secretariat**. Mr. Vigneault noted that, while DI did not necessarily receive intelligence reports, it led the policy effort

to protect democratic institutions against FI and safeguard electoral processes. Mr. Vigneault identified the NSIA and PCO SI as the branches with which PCO had an operational relationship.

e. SITE TF

Ms. Tessier indicated that, when SITE TF was stood up, CSIS had a dedicated taskforce to determine which information would be disseminated to SITE TF. Ms. Henderson stated that the threshold for bringing information to SITE TF was low, as the objective was to ensuring that all information was available to SITE TF.

The witnesses were asked to comment on the following documents:

1. A Report;
2. An email from the then-head of the SITE TF and a CSIS employee dated November 1, 2019 raising concerns regarding the timing of the dissemination of the Report referred to at point 1;
3. A corrected version of the Report referred to at point 1 which removes the sentence quoted above.

Ms. Tessier's recollection was that the intelligence underlying the Report would likely have been shared with SITE TF. The activities of this actor did not impact the integrity of the election as a whole, which is why the correction was then made. She agreed that the choice of wording in the Report could have created some confusion and that this is what may have prompted the email from the then-chief of the SITE TF.

Ms. Henderson agreed with Ms. Tessier's assessment that the individual may have had a limited impact on the election, without the integrity of the election as a whole having been compromised.

Mr. Vigneault stated that this was an illustration of the problem with SITE TF's more intensive activities being limited to the writ period. Indeed, SITE TF would not have been provided with intelligence that was disseminated outside of the writ period. Since FI activities are much bigger than electoral interference and generally take place over a long period of time, focussing mainly on the writ period may result in information gaps. Mr.

Vigneault also emphasized, as did Ms. Henderson and Ms. Tessier, that FI during an election does not necessarily compromise the election's integrity as a whole.

f. P5

Mr. Vigneault, who briefed the P5 on a number of occasions, indicated that the P5 was, generally speaking, provided with a distilled version of the information provided to the SITE TF. The P5 also received SITE reports directly from SITE. CSIS would typically choose which products would be brought to the attention of the P5, and P5 would sometimes then ask questions, or for further intelligence products on a specific issue. Mr. Vigneault described this mechanism as effective.

g. Cabinet Ministers

Mr. Vigneault explained that the briefing of Cabinet, as a whole, was coordinated by PCO.

He added that any briefing of the Minister of Public Safety [the minister responsible for CSIS] could be conducted at the initiative of Public Safety or of CSIS, sometimes with the input of Public Safety where the subject-matter of the briefing was particularly sensitive. For individual briefings of other ministers, CSIS would contact their chief of staff.

h. Prime Minister

The briefings to the **Prime Minister ("PM")** would be delivered by the Director. They could be initiated at CSIS' initiative (*e.g.*, in the case of a very serious threat), but were mostly conducted at the request of the NSIA, the PCO Clerk or PCO more generally.

As examples, Mr. Vigneault identified the following briefings delivered to the Prime Minister:

1. On February 9, 2021, Mr. Vigneault briefed the PM on FI. Commenting on this briefing, Mr. Vigneault explained his practice was not to bring any unconfirmed intelligence to the attention of the PM.

2. In September 2022, Mr. Vigneault briefed the PM on FI at the request of the Clerk of the Privy Council.

3. In November 2022, following leaks of alleged CSIS information in the Canadian media, Mr. Vigneault briefed the PM in the presence of the Clerk, the NSIA, the Assistant Secretary of IAS, the Foreign Defence Policy Advisor, as well as three or four senior employees of the **Prime Minister's Office ("PMO")**.

Responses to FI

Threat Reduction Measures ("TRMs")

Ms. Tessier explained that TRMs are initiated by the intelligence officers overseeing a given threat, either from a CSIS regional office or from CSIS HQ, before going through the approval process. This involved consultation with partners for the analysis of the following four risk pillars, as set out in the Ministerial Direction for Operations and Accountability (2015) and the Ministerial Direction for Accountability (2019):

1) operational risk;
2) foreign policy risk in consultation with GAC;
3) legal risk in consultation with Justice Canada; and
4) reputational risk – previously CSIS assessed this alone but now consults Public Safety in conducting this assessment.

Ms. Tessier also pointed out that CSIS must consult the RCMP for all TRMs. She noted that, while the RCMP and other departments listed above did not have a veto over TRMs considered by CSIS, if they advised CSIS that the proposed TRM would have an important adverse effect on their operations, CSIS would usually not initiate it.

Ms. Tessier added that, in order to build expertise on this specific matter, the assessment and coordination of the consultation process relevant to all TRMs was led by the TRM Unit. The final level of approval required to initiate a TRM depended on the level of risk assessed. TRMs that were considered low risk could be approved at the operational level. TRMs with a medium risk could approved at the Deputy Director General level, whereas high-risk TRMs must be approved by the Minister.

Mr. Vigneault explained that the monitoring of ongoing TRMs was led by CSIS. The National Security Review Agency ("NSIRA"), is notified of all TRMs pursuant to ss.

12.1(3.5) of the *CSIS Act*. The Minister of Public Safety was informed of all TRMs as per ss. 6(5) of the *CSIS Act*.

Security Briefings

The witnesses were asked to comment on Appendix B of CSIS' Institutional Report [Appendix B is a classified list of protective security briefings ("PSBs"), sometimes referred to as defensive briefings, given to elected officials, related to the threat or incidence of foreign interference in the 43rd and 44th federal elections and Canadian democratic institutions].

Ms. Tessier noted that CSIS had wanted to conduct such briefings even before the 43rd elections and before the National Security and Intelligence Committee of Parliamentarians formally recommended it. She explained that ultimately, CSIS prioritized briefing those Members of Parliament who were vulnerable to potential FI activity.

Ms. Tessier drew a distinction between briefings conducted under TRM authority and those that are not. Briefings conducted under a TRM authority allow CSIS to disclose classified information and to be much more specific in the information they share. Security briefings not conducted under TRM authority would inform potential FI targets of the threat in general terms as well as means to mitigate the FI activity.

Ms. Tessier and Mr. Vigneault expressed CSIS's willingness to conduct more of these types of briefings, which they viewed as highly effective to raise awareness. Ms. Henderson added that these briefings also created opportunities for further engagement with individuals.

Challenges

In regards to security briefings, Ms. Tessier noted that the requirement to have a TRM approval to disclose classified information in a PSB to members of political parties was time consuming and laborious. It was her view that the *CSIS Act* should allow CSIS to have greater flexibility for providing individuals with specific threat-related information. Mr. Vigneault added that, as a TRM must necessarily serve to reduce a threat, this mechanism may not cover all briefings given to members of political parties. He also explained that s. 19 of the *CSIS Act* limited CSIS's ability to disclose classified information and that, as a result, CSIS needed to find creative ways of alerting potential victims of FI.

With reference to [notes from a briefing delivered to the cleared representatives of the Liberal Party of Canada regarding PRC FI during the 44th election], the witnesses explained that briefings to political parties had limitations. Indeed, Mr. Vigneault noted that the government had already been briefed on this issue, but that briefing a governing political party during the writ period could give rise to independence issues if the target of FI is a member of an opposing party. Ms. Tessier added that CSIS had limited visibility over the actions taken by political parties based on the information that they were provided with.

Mr. Vigneault indicated that the P5 had been created to address these challenges during the writ period, but also noted that it could not intervene on FI incidents that did not meet its threshold for action or that occurred outside the writ period. Mr. Vigneault suggested that the United Kingdom and Australia had ways of engaging political parties on a more frequent basis from which Canada could draw inspiration.

Mr. Vigneault noted that an effective way of countering FI was to publicly call out actors on their activities in the diplomatic sphere, as this requires them to operate more covertly and, in all likelihood, less effectively, but that such measures were complicated to put in place. Ms. Tessier agreed and added that she perceived that, while some actors would stop their activities when informed by CSIS that it is aware of their FI activities, others considered that they could conduct FI openly, without any consequences. She and Mr. Vigneault emphasized that CSIS utilized all the available tools under its mandate, but that this was sometimes ineffective, (*e.g.* because not all individuals are always receptive to CSIS briefings).

Ms. Tessier indicated that, considering the limited effectiveness of the tools available specifically to CSIS, and because FI is a multi-faceted threat, it was necessary to have a "whole-of-government" approach to effectively counter it. Mr. Vigneault agreed and noted that there was a concerted effort within government to help achieve this (*e.g*, standing up senior inter-departmental committees to address the threat of FI), but that there remained challenges to ensure that intelligence could be acted on within government. Mr. Vigneault noted that the Counter Foreign Interference Coordinator, a position created in 2023 and housed in Public Safety, was a good step in that direction. Ms. Henderson added that

another example was the interdepartmental group that was brought together further to the "Police Station issue", to determine tools under all departments' mandates to address that threat.

Specific incidents of FI linked to the 43rd and 44th General Election

CSIS subject of interest

The witnesses were asked to comment on an email exchange in December 2022 regarding a proposed TRM.

The witnesses noted that the reporting on the subject of interest and the differing views in the assessment of the intelligence from the relevant regional office and CSIS Headquarters, were an example of the different perspectives of Headquarters and Regional Offices. Mr. Vigneault added that he had expressly indicated that he was receptive to personally assessing any level of investigative activity against the subject of interest despite the sensitivity of the investigation.