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

Supplementary *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 an *in camera* hearing held in August 2024. 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 effective July 20, 2024 and is concurrently its Deputy Director of Operations **("DDO")**. She was appointed to that position in May 2023. Prior to that, 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 of CSIS from December 2018 until March 2023, when she retired after 35 years with CSIS.

[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 Director General of the Intelligence Assessment Branch (“**IAB**”) of CSIS from 2019 to 2021. In that capacity, she oversaw the production and dissemination of intelligence reports. She was acting Assistant Director, Requirements (“**ADR**”) from 2021 until her appointment as ADR in 2022, and remained ADR until her retirement from CSIS in 2024.

2. Examination by Commission Counsel

2.1 Specific Cases of FI

[6] Mr. Basler was asked about Instance Number 1 in the Classified CSIS Stage 2 Institutional Report (“**Classified CSIS IR**”) which corresponds to bullet point number two in the unclassified CSIS Stage 2 Institutional Report.

[7] Commission Counsel asked whether CSIS had briefed political officials on the related intelligence. Mr. Vigneault had no recollection of this being done and did not believe that this information had ever been briefed to the political level.

[8] Commission Counsel asked questions about Instance Number 6 in the original Classified CSIS IR.[1] The witnesses indicated that the related intelligence had been distributed to appropriate Government officials.

[9] The witnesses noted that both instances, mentioned above, were briefed to the Minister of Public Safety and other ministers in briefings held subsequent to media leaks in 2023.

[10] The witnesses were asked about a proposed TRM from 2023 that was not implemented. Mr. Basler explained there was considerable internal discussion within CSIS about how to operationalize the Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians (the “**Directive**”). At a very basic level, CSIS was reviewing its holdings to determine which Members of Parliament

[1] Please see Footnote 1 to the *In Camera Examination Summary: Canadian Security Intelligence Service Senior Officials* [WIT0000134]. Instance Number 6 in the original Classified CSIS IR is the one that was subsequently removed from the list of Significant Instances of Suspected Foreign Interference

(“**MPs**”) were referenced, determining whether the information in their holdings constituted a threat to the MP, and then deciding what could be done in accordance with the Directive. CSIS considered resorting to its threat reduction mandate under the *CSIS Act*, as it had previously used a TRM to convey FI information to affected MPs. Accordingly, another TRM was considered to address ongoing threat activity but, as events unfolded, it was determined that such a measure was not the right mechanism, at least not in 2023, and, as a result, it was not pursued.

[11] The witnesses were then asked about potential Iranian FI activities directed at the Iranian diaspora in Canada. The witnesses were asked about allegations made in the media by Kaveh Shahrooz, an Iranian Canadian lawyer and vocal critic of the Iranian regime, that Iranian officials had interfered in a nomination process in which he had sought to be a candidate. Mr. Basler noted that CSIS was aware of Iranian threat-related activities in Canada including activity within the Iranian diaspora community but that Iran has not historically been a significant FI threat actor at the national or electoral district levels.

[12] Ms. Henderson provided additional information about Iran and its FI activities. Its focus has not been on influencing democratic processes, but primarily on influencing Canadian and global responses to the downing of Flight PS752 and Iran’s role in it. For example, threatening persons in the Iranian diaspora community who are vocal critics of Iran’s role in the downing of the plane.

2.2 Briefings to Parliamentarians

[13] The witnesses described the various types of briefings to Parliamentarians that could be delivered. [The first type of briefing is a broad unclassified briefing to Members of the House and Senate. This briefing for Members, would be delivered upon their being sworn in and regularly thereafter. This was recommended in the National Security and Intelligence Committee of Parliamentarians’ (“**NSICOP’s**”) 2018 Special Report into the allegations associated with Prime Minister Trudeau’s official visit to India in February 2018, and reiterated at paragraph 126 of NSICOP’s unclassified Special Report on Foreign Interference in Canada’s Democratic Processes and Institutions (“**NSICOP**

Report”). The possibility of delivering this type of briefing was discussed at various levels within government but, for various reasons, no action was taken to give effect to the NSICOP recommendation.]

[14] With respect to briefing Parliamentarians about security matters, the witnesses were asked to comment on their understanding of the division of responsibilities between government security agencies and the Houses of Parliament. Mr. Vigneault indicated that the primary responsibility for House of Commons security rests with the Sergeant-at-Arms and, with respect to Senate security, with the Usher of the Black Rod. He noted that, while CSIS has the authority to brief individual MPs, it would be highly unusual for CSIS, CSE or the RCMP to brief MPs as groups (*e.g.*, by caucus) and there would not really be a mechanism for it without first going through the Sergeant-at-Arms. According to custom and past practice, when an agency handles a matter that involves the Houses of Parliament, it also involves the Privy Council Office **(“PCO”)**. This is the procedure that was followed when Mr. Vigneault was at PCO and there was an attack against Parliament in 2014. There is no relationship between government agencies and the Houses of Parliament independent of PCO, and Mr. Vigneault agreed with Commission Counsel that there was no mechanism whereby CSIS can deliver unclassified briefings to groups of MPs.

[15] Mr. Vigneault and Mr. Basler described the steps that CSIS took to respond to the above-noted NSICOP recommendation. Mr. Vigneault discussed the challenges in communicating information to MPs and described the development of a multidisciplinary (CSIS, CSE, the Royal Canadian Mounted Police (“**RCMP**”), and Public Safety Canada (“**PS**”) approach to MP briefings at the unclassified level, which was coordinated by PS and the Sergeant-at-Arms. The content of the briefing was in keeping with the spirit of the NSICOP recommendation. Mr. Vigneault noted that he was personally aware that requests were made to the Prime Minister’s Office to authorize delivery of the briefings. He noted that NSICOP appeared to have accurately described his perception of this sequence of events and agreed with Commission Counsel that the decision that the Prime Minister’s approval was required before the briefings could be delivered was PCO’s.

[16] Mr. Basler testified that, regarding the initiation of the June 2024 unclassified briefings, there were a few parallel conversations going on simultaneously. In the summer of 2023, the Sergeant-at-Arms of the House of Commons reached out to the Service's National Capital Region office and asked the Service to brief the political parties. Mr. Basler stated that the Service could have provided the unclassified briefings on its own, but it wanted a community briefing to occur because of the heightened attention that was being paid to the matter across parties. The Service engaged PS through the Office of the National Counter-Foreign Interference Coordinator and provided the material the Service had compiled for the briefings. The Service thought PS should lead the effort so it would be a Government of Canada combined effort. PS agreed and took the Service's initial presentation material and engaged with CSE and the RCMP to create new material.

[17] Mr. Basler testified that in the summer of 2023 they did a few dry runs of the briefing to make sure it was on point. This included a dry run with staff from the Minister's office. However, this was happening immediately prior to the House recess, and there was no opportunity before the break to get all caucuses together to provide the briefings.

[18] Mr. Basler explained that the briefing effort started again in the fall. The Sergeant-at-Arms came back to the Service's National Capital Region ("**NCR**") office to request the unclassified briefings. In June 2024 the briefings were delivered. The briefings occurred caucus by caucus so that parliamentarians from each party could ask questions without another political party being present. Mr. Basler attended the briefings with a representative from PS, a representative from the RCMP, and a representative from the Canadian Centre for Cyber Security ("**CCCS**"). The content of the briefings mirrored the type of information that the Service provided in protective security briefings: what constitutes FI, why states conduct FI, and some examples of FI activities. The briefing was high level and intended to provide a baseline understanding for all MPs.

[19] Mr. Vigneault testified that one of the objectives in sharing high level information was to help the MPs generate questions so that they could have more precise conversations with the Service. Mr. Vigneault added that while the Sergeant-at-Arms had contacted CSIS' NCR office, he had also contacted Mr. Vigneault directly to reinforce his request

for briefings. Mr. Vigneault told the Sergeant-at-Arms that the Service could not provide the briefings unilaterally. This issue was not only discussed at the operational level, but at the Deputy Minister level as well. Mr. Vigneault discussed with his colleagues, including the Deputy Minister of Public Safety and the members of the Deputy Minister Committee on Intelligence Response (“**DMCIR**”), and told them that they needed to find a way to respond to this request of the House of Commons for a briefing.

[20] Mr. Basler testified that the briefings seemed well received. The Service received positive comments. About 50 to 60% of each caucus showed up, except for the Green Party of Canada whose sole caucus member attended. There was engagement and a number of questions from the MPs during the presentations. Each agency told the MPs to reach out through the Sergeant-at-Arms if they had subsequent questions. One of the political parties asked for follow up.

2.3 Classified briefings

[21] Commission counsel referred the witnesses to a document [on May 1, 2023, there was a media leak about the PRC targeting Michael Chong. On May 2, 2023, at the request of the Prime Minister, CSIS conducted a TRM under exigent circumstances to brief MP Chong. This document is the implementation report of the Director’s brief to MP Chong under the TRM]. Mr. Vigneault testified that Jody Thomas, the National Security and Intelligence Advisor to the Prime Minister (“**NSIA**”), was also present at the briefing. MP Chong was very receptive to the briefing. He was very professional and there was no tension during their discussion.

[22] Commission counsel referred the witnesses to CAN013134 [this document summarizes various engagements between the Service and MP Chong]. Mr. Vigneault testified that this information was compiled because of the perception of some individuals in Government and in the public that MP Chong was unaware of PRC threats directed towards him and that the leak was the first time MP Chong was apprised of the information concerning him. As indicated in the document, the Service met with MP Chong several times [prior to the leaks]. These interactions were unclassified but informed by CSIS representatives’ knowledge of the full, classified picture, which

allowed them to properly contextualize the unclassified information. The interactions with MP Chong were positive. MP Chong was a person who had thought a lot about FI. On other occasions, MP Chong himself contacted CSIS to have further conversations and share information with the Service. It is that context that preceded the May 2, 2023 TRM with MP Chong.

[23] Ms. Henderson added that the Service knew there was PRC interest in MP Chong so they set up a protective briefing with him. These briefings are intended to provide the MP with awareness of what is happening and are also an opportunity to hear what the MP may have experienced. The Service had also interacted several times with him prior to Mr. Vigneault giving the briefing under the TRM at the direction of the Prime Minister.

[24] Ms. Henderson further stated that, as part of Mr. Vigneault's briefing to MP Chong, he sought to correct what is meant by "target". The allegations referenced in the media reporting say "target", but what that means is primarily an individual of interest, not necessarily that the individual is a target for violence. It can mean a lot of things, for instance a "target" of FI, and not necessarily that CSIS believes violence or harm may be perpetrated against the individual. In some cases, target can mean harm, but harm does not necessarily mean harm through violence. This harm can include, for example, threats that prevent the person from travelling to the PRC.

[25] Commission counsel referred the witnesses to a memorandum to the Minister dated May 18, 2023 and titled "Threat Reduction Measure: Targeting Specific Members of Parliament".[2] Mr. Basler explained that the Director had delivered the briefing to Mr. Chong under exigent circumstances without going through the usual risk assessment and approval process. He explained that CSIS still needed to inform the Minister and seek his approval. This TRM had an elevated level of risk including high risk ratings in the reputational and foreign policy risk assessments.

[26] Commission counsel referred the witnesses to a document where CSIS is seeking ministerial approval to brief a small group of MPs under a TRM. Mr. Basler indicated that, after the briefing to Mr. Chong, CSIS looked at its holdings to identify other affected

[2] CAN012593.

Parliamentarians, in light of the fact that the Directive would soon be issued. This Directive was directly related to the briefing to Mr. Chong. CSIS identified other MPs who were of heightened interest to the PRC like Mr. Chong. Those MPs included Mr. O'Toole, Ms. Kwan, and Mr. Chiu. CSIS decided that it would deliver the same type of briefing to these MPs, with content specific to each of them. These TRMs also had the same elevated level of risk. As per the Directive, CSIS sought ministerial approval to undertake the TRM. They became the first MPs to be briefed under the Directive.

[27] Commission counsel referred the witnesses to page 2 of a PCO memorandum to the Prime Minister dated September 8, 2023 and titled "Update – Upcoming Threat Reduction measure Briefings to Parliamentarians":[3]

> • On May 16, 2023, the Minister of Public Safety issued a Ministerial Directive on Threats to the Security of Canada Directed at Parliament and Parliamentarians **(TAB A)**. The Minister directed CSIS, wherever possible, to "ensure that parliamentarians are informed of threats to the security of Canada directed at them."
>
> • Following this Ministerial Directive, CSIS identified parliamentarians to whom individualized threat information should be disclosed. CSIS conducted three TRM to disclose threats to Michael Chong (on May 2) and to Jenny Kwan and Erin O' Toole (on May 26).
>
> • Following Mr. O' Toole's speech in the House of Commons on May 30 (**TAB B)**, Public Safety Canada (PS) and CSIS paused further disclosures to parliamentarians in order to develop a governance protocol through which the security and intelligence community would have the opportunity to review CSIS' key messages for disclosure and the intelligence on which they are based.

[28] In response to a question from Commission counsel about the impact of Mr. O'Toole's speech on the process of the Independent Special Rapporteur **("ISR")**, Mr. Basler explained the process the ISR had followed was very different from that of the Public Inquiry into Foreign Interference, or from that of either of CSIS' two review bodies. The ISR sought information about threats generally and then focused on specific threats, about which he sought additional information, documentation, and presentations. One of the major focuses of the ISR was the media leaks, and the damage they were causing to Canada's fundamental institutions, as well as the erosion of trust in these institutions caused by the leaks.

[3] CAN028170.

[29] Based on conversations that Mr. Basler had had with the ISR's team, he believed that the ISR wanted to focus on the individual allegations that had been reported by the media following the leaks. After the ISR laid down the general context around FI and the threat activity, his investigation focused on those allegations. As a result, CSIS did not present, in all cases, every single piece of intelligence they had on FI to the ISR. CSIS presented information in response to the ISR team's lines of questioning. The ISR and his team did not seek the production of all products related to FI over a defined period and, as such, the process did not have a broad collection of documents that informed their lines of inquiry from the outset.

[30] Mr. Basler explained that what CSIS shared with Mr. O'Toole, under the Directive, was information which had not been shared with the ISR. The gap was not large. CSIS did not present to the ISR intelligence that was either not credible, not sourced, or not pertinent to the line of inquiry he was pursuing. When CSIS briefed Mr. O'Toole, it provided all information, with the appropriate qualifiers, because the wording of the Directive meant CSIS had to brief everything. This briefing was verbal, and Mr. O'Toole could not take notes, so his recollection is what it is. Mr. Basler did not attend the meeting with Mr. O'Toole but he believed it lasted over an hour and included a lot of information. The problem that arose was that the details that were shared by Mr. O'Toole in his public speech did not accord with the understanding of the ISR. The ISR team came back to CSIS and asked about the discrepancy. CSIS attempted to identify the intelligence that Mr. O'Toole was likely referring to from his briefing, and presented it to the ISR. After that process was completed, the ISR had all the information, but Mr. Basler indicated it informed his decision on going forward.

[31] Mr. Vigneault explained that, following the leaks and the reactions of the media and MPs to the targeting of an MP by the PRC, the government conducted an internal investigation to determine the flow of information. The Prime Minister publicly announced that he would issue a directive to CSIS to ensure that all information was available to those who needed it. Mr. Vigneault noted that in practice it was the Minister of Public Safety who has the relevant authority to issue such a directive.

[32] Mr. Vigneault testified that discussions then began with Public Safety about the Directive and that CSIS expressed concerns about the content of the draft Directive. Although the Deputy Minister assured Mr. Vigneault that he could speak to the Minister before the Directive was issued, the Minister issued the Directive the next day, unchanged, including with the issues that CSIS had identified as being problematic. It is under that Directive that Mr. O'Toole was briefed for the first time. Mr. O'Toole subsequently spoke in the House of Commons and shared some classified information which had been disclosed to him during the TRM. Mr. Vigneault considered parts of Mr. O'Toole's public comments inaccurate, though recognized that Mr. O'Toole could not take notes during the briefing and so what he delivered in House of Commons was based on his memory. This placed the government in a difficult situation, because people were wondering why they had not been previously made aware of some of the information Mr. O'Toole was sharing.

[33] Mr. Vigneault explained the purpose for creating the Governance Protocol that followed Mr. O'Toole's speech in the House [referred to in the memorandum to the Prime Minister]. The Protocol was meant to correct issues with the Directive, namely the fact that it required CSIS to disclose *all* information that it had collected with respect to threats to parliamentarians, regardless of whether the information was corroborated, verified or credible. For CSIS, this was not at all an advisable approach. In the case of Mr. O'Toole, CSIS briefed the MP in a way that respected the Directive but people in government ultimately understood this to be unworkable. The government paused the briefings and decided to revise the implementation of the Directive through a Protocol.

[34] Ms. Henderson explained that it had become abundantly apparent that all stakeholders needed to be engaged to discuss what CSIS would share and provide in the briefings to parliamentarians. A process was therefore developed further to which an operational CSIS team would pull the relevant information, draft the discussion points that CSIS would be raising, and provide the "facting" ["facting" is the process by which the relevant underlying intelligence is identified] behind these points. Ms. Henderson's office would then share these materials with her counterparts.

[35] Ms. Henderson noted it is a small intergovernmental Assistant Deputy Minister group doing this work, consisting of officials from Public Safety Canada, CSIS, CSE, PCO and

GAC. It was created specifically for this function because of the sensitivity of the information underlying the briefings. Each of those departments would receive and review the package, including the speaking points and the "facting". CSIS would then hold another meeting to discuss everything so that the other departments could raise any concerns they had. Following that meeting, if there were no concerns, this would be provided to DMCIR**.** That Committee would review the information and, if it supported it, CSIS would proceed with the briefing.

[36] Commission counsel referred to page 15 of the memorandum to the Prime Minister, which reads, in part:

> **Modification for conflicts of interest**: Public servants, exempt staff, and Ministers operate in and around Parliament. There is a risk that individuals involved in this process have an interest in the outcome. From time to time, adjustments to the protocol may be needed to limit distribution of a document or otherwise modify a step to avoid real or perceived conflicts of interest. If CSIS identifies such a concern, they will raise it with Public Safety Canada for agreement on the revised process for that specific instance.

[37] Mr. Vigneault indicated that he did not have a recollection of specific discussions on this point. This part of the protocol was not used during his tenure. He speculated that, since members of the government are also members of a political party, in some specific cases, CSIS might end up providing information that could, theoretically, be used for political purposes. He indicated that this paragraph may have been designed as a safeguard to ensure that the Governance Protocol would not be implemented without consideration of the risk of conflicts of interest. Ms. Henderson agreed with Mr. Vigneault and noted that one of the challenges that CSIS faced in its investigations of, and engagements with, the political sphere is that they involve a very unique group, whose members know each other quite well. In some cases, a minister might be asked to approve a warrant application involving an MP from another party. Since the Governance Protocol provides that the members of DMCIR would advise their respective ministers that a briefing would occur, CSIS also wanted to have the option for another way forward in cases where there could be a potential conflict of interest (*e.g.*, the DMCIR members would not advise the relevant ministers). The idea was to try to foresee and avoid any possible conflict that might arise. Ms. Lloyd added that, under the Governance Protocol, the proposed briefing is brought to DMCIR not for approval, but for consultation. The members of DMCIR can provide

advice to the Director with respect to the execution of CSIS authorities that the Director seeks to exercise.

[38] Mr. Basler then confirmed that the first briefing that occurred under the Governance Protocol was to Kenny Chiu in September 2023.

2.4 APT31

[39] Commission counsel referred the witnesses to a document which states that:

> APT 31 is known to target government officials; however considering the current diplomatic situation between Canada and the PRC, [text deleted] this event [the targeting of certain government officials] is possibly an outcome of PRC threats of increased activities against Canada.

[40] Ms. Henderson indicated that, while this was before her appointment as ADR, the CCCS has the lead on these situations. If there is a cyber attack that originates from outside the country and targets Canadian institutions, the first line of response, and the first entity to launch an investigation, is the CCCS. CSIS supports and assists the CCCS, and can, under the *CSIS Act*, conduct a retrospective investigation to determine from where the threat actor originated. The CCCS, however, is the lead department responsible for stopping the attack, determining what happened, and identifying who was attacked. The CCCS sometimes receives assistance from the Royal Canadian Mounted Police. The community has been working hard to establish cohesion between the Service's cyber team, CSE, and the RCMP, and to educate all partners on their respective roles. Ms. Henderson noted that, before the creation of the CCCS, CSIS was undertaking a lot of this work, but now CCCS has this mandate.

[41] Commission counsel referred the witnesses to a classified CSIS Analytical Brief from November 2021 on the topic of a tracking link campaign targeting members of the Inter-Parliamentary Alliance on China ("**IPAC**") by PRC cyber threat actor, APT31. The document included information that the campaign had been deemed unsuccessful. The intention of the tracking link campaign could have been to gain insight into the work of IPAC members and/or to gather information about IPAC members for the purpose of embarrassing or discrediting them.

[42] Mr. Vigneault explained that, when the information [about the cyber campaign targeting members of the Inter-Parliamentary Alliance on China] first became known, agencies began to communicate with each other as a matter of process. In this case, the CCCS, and CSIS sought to understand the information that was emerging. It was decided that the CCCS would [take the lead and] speak with the Sergeant-at-Arms to inform them of what had happened. CSIS was present at many of these meetings and also spoke separately with the Sergeant-at-Arms. It was decided that the Sergeant-at-Arms would do any follow up required.

[43] Mr. Vigneault noted that, when some of this information became public, it was debated before Parliamentary Committees, because parliamentarians wanted to know why they had not been informed. Mr. Vigneault indicated that CSIS had initially been blamed for this, as it was subject to the Directive. However, he noted that it was very clear that primary responsibility was with the CCCS and they were the ones who had followed up [with the Sergeant-at-Arms] as necessary. He indicated that CSIS had contributed to follow up efforts. Mr. Vigneault believed that the takeaway from that event was that there should have been discussions with the office of the Sergeant-at-Arms regarding what had been done [with the information]. He noted that this event occurred in a context where staff were mostly working remotely because of the COVID-19 pandemic. Mr. Vigneault further stated that, as he told PROC, the committee should recommend that the relevant agencies take part in a table-top exercise to help them understand their respective roles and responsibilities, and how similar issues could be better addressed moving forward.

[44] Ms. Henderson noted that, in these cases, CSIS continues to investigate the cases and speak with Canada’s allies. CSIS also continues to draft analytical products to inform government about the threats to national security. While CCCS continues to have the lead on these types of events, CSIS is always available to support CCCS and collect information to bring out a more complete picture of the threat.

[45] Mr. Vigneault and Ms. Henderson both indicated that, in order to defend against this threat actor, a fairly detailed understanding of its tactics was necessary. Ms. Henderson specified that, if one wanted to give information to a parliamentarian regarding the

means they could take to protect themselves against this type of threat, the information could be high-level. Conversely, if one wanted to provide information to the protective services that are in charge of protecting the devices of parliamentarians, the level of detail provided would need to be higher.

[46] Mr. Basler noted that the Directive is not retroactive: if a threat no longer persists, the Directive does not apply. He said that, now that the Directive is in force, whether it would apply if a similar issue arose is open for debate, including with respect to which agency would have the lead in terms of responding.

[47] Mr. Basler stated that, because this event involves a cyber security threat against the House of Commons, CCCS would have the lead. The debate as to whether the parliamentarians should be informed, and who would lead this, would be between CCCS, CSIS, as well as the House of Commons information technology security. He considered that it was not currently clear that the Directive engages CSIS if CSIS does not generate or discover the intelligence regarding the threat. CSIS has committed to making sure that, if it learns of a threat [through other means than its own collection activities], even if CSIS is not the one directly informing parliamentarians about it, they will live by the spirit of the Directive and ensure that this conversation is happening. Mr. Basler added that, if CSE informs CSIS of a threat against Parliament, CSIS will ensure that there is a discussion to determine whether parliamentarians should be informed, and by whom.

[48] Ms. Lloyd specified that, in the case of a cyber incident directed at parliamentarians, there is an established role for the CCCS to engage with the Sergeant-at-Arms. She noted that the Directive only applies to CSIS. She explained that, at present, if SIGINT detects a threat that relates to a different type of FI (not a technical attack, as in the case of APT31), and CSIS is aware of that report, CSIS has the mandate to share that information. CSE would also expect CSIS to share this information, as required by the Directive. Ms. Lloyd noted that there is an active discussion at DMCIR to determine whether the scope of application of the Directive should be broadened to the whole national security community, to account for the fact that CSIS is not the only producer of intelligence related to threats. While it is clear that CSIS has the authority to engage

with parliamentarians about these threats, there is less clarity with respect to the authority of other departments to engage directly, although CSE does have some authority.

[49] Mr. Vigneault noted that his suggestion to do a table-top exercise could address the uncertainty about the applicability of the Directive and the mandates of the various agencies (Sergeant-at-Arms, CSE, CCCS) involved. Examining a practical case could lead to greater clarity and identification of existing gaps. The government could then fix these gaps.

2.5 National Security Governance in Canada

[50] Mr. Vigneault explained that the Service has a very specific role within the FI space and is only one of the players within the security and intelligence community. The comments he made during the October 12, 2023 DMCIR meeting[4] are still relevant insofar as there is an ongoing evolution and there remains much to do with respect to national security governance. The role of the National Foreign Counter-Interference Coordinator ("**NCFIC**") has been announced publicly but the daily work of the Coordinator and the development of their leadership in this space is still evolving. The NSIA gave her opinion at this meeting that the NCFIC should be housed at PCO rather than at PS. These questions are still under discussion. The role of the NCFIC and their leadership in this space did not evolve as quickly as we would have wanted it to. This is the spirit in which these comments were made.

[51] Mr. Vigneault pointed to the briefing that was delivered to MPs, caucus-by-caucus in June 2024, and which was coordinated by the NCFIC as an example of positive evolution of national security governance. Work is still required to find ways of making intelligence more actionable. The mechanisms available to do this are not yet agile enough. Having discussions between DMs on a piece of intelligence is not sufficient to determine how the community will actually respond to that intelligence. Bill C-70 will be a good opportunity to encourage actors in this space to consider their respective roles and responsibilities,

[4] CAN044228.

for instance, the RCMP's role in prosecuting the criminal aspects of FI. Mr. Vigneault reiterated testimony he has previously given in public and in private: threat actors commit acts of FI in Canada because they believe there are no consequences. The judicial developments and the new offenses created under Bill C-70 will allow both the RCMP and the Service to find the intelligence that will enable more responses to FI. Mr. Vigneault stated that he hopes the Commission's recommendations will be able to help more quickly advance governance with respect to FI. The right people are now sensitized to, and seized with, the issues; additionally, there is institutional interest in addressing the issues. That said, Mr. Vigneault believes that to protect Canadians from FI, we have to continue to evolve because the system is not yet mature enough to fully counter FI and dissuade threat actors.

2.6 Questions from the AGC

[52] Ms. Lloyd described some of the improvements made to the "flow of information" within and from CSIS. There were discussions at DMCIR to determine how the community could make improvements to track the dissemination of intelligence and ensure that consumers receive intelligence. Intelligence products of the broader community, including CSIS, are housed on CSE's new system database. The platform allows the Service to track where intelligence has gone, to whom it was disseminated and to capture more feedback and actions on those reports.

[53] The Service has supplemented this change by deploying intelligence dissemination officers. This ensures that senior officials within the Service's portfolio have a special service. The Service now has the ability to sit with those that receive intelligence, provide verbal briefings, and come back on any questions the recipient might have. There is another intelligence dissemination officer serving departments within the community where the Service has some value to add or where the department has responsibilities where intelligence is relevant to fulfilling those responsibilities.