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: Privy Council Office – Security and Intelligence Secretariat, Intelligence Assessment Secretariat (Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald, Martin Green, Lisa Ducharme)

Senior officials from the Security and Intelligence Secretariat ("**S&I**") and the Intelligence Assessment Secretariat ("**IAS**") at the Privy Council Office ("**PCO**") were interviewed by Commission Counsel in a panel format on June 19, 2024. The interview was held in a secure environment and included references to classified information. This is the public version of the classified interview summary that was entered into evidence in the course of hearings held *in camera* in July and August 2024. It discloses the evidence that, in the opinion of the Commissioner, would not be injurious to the critical interests of Canada or its allies, national defence or national security.

Notes to Readers:

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

1. Witnesses

1.1 Intelligence Assessment Secretariat

[1] Lisa Ducharme is the Director of Operations at IAS. She joined PCO in March of 2023, and previously held roles in Royal Canadian Mounted Police ("**RCMP**") intelligence, at the Department of National Defence ("**DND**") and Public Safety ("**PS**"). As Director of Operations, she handles day-to-day operational needs at IAS. This includes intelligence assessment product support, information flow, staffing, finance, and Access to Information and Privacy ("**ATIP**") requests. She also spearheads the Canadian

Academy for Intelligence Analysis, a body that provides intelligence training, and the Intelligence Analyst Community of Practice that sets out standards of practice for intelligence analysts. In her capacity as Chair of the Director General Intelligence Assessment Coordination Committee ("**DG IACC**"), she serves a leadership and coordination role across the intelligence assessment community, planning the production of assessment products, and coordinating the preparation of joint assessment products. This includes both topic-specific products and broader products like the National Security Outlook, which is put out annually. Ms. Ducharme served as Acting Assistant Secretary of IAS from February 2024 until July 5, 2024, acting for Mr. Martin Green when he was not available.

[2]   Martin Green was the Assistant Secretary at IAS. He retired effective July 5, 2024. As Assistant Secretary, he reported to the National Security and Intelligence Advisor ("**NSIA**") to the Prime Minister.

[3]   IAS provides policy-neutral, all-source strategic assessments that incorporate both overt and covert foreign intelligence. It has a large product line, which includes National Intelligence Assessments, intelligence profiles on foreign leaders, placemats, and other reports. The Assistant Secretary of IAS serves as Chair of the Assistant Deputy Minister Intelligence Analysis Committee ("**ADM IAC**") [a committee that reviews intelligence assessments], which previously supported the Deputy Minister Intelligence Assessment Committee ("**DMIA**"), later the Deputy Ministers' Intelligence Committee ("**DMIC**") [a committee that considers the IAS-assessed long pieces on future strategy from a policy perspective, and flags important intelligence assessments to deputy heads], and now provides contextual support to the Deputy Ministers' Committee on Intelligence Response ("**DMCIR**") [DMCIR is a committee created by the NSIA to facilitate the identification of relevant actionable intelligence, to coordinate decisions on how to best respond with operational, enforcement or policy action, and to triage the intelligence to be briefed to Cabinet].

[4]   IAS also helps to coordinate the intelligence assessment community, both domestically (i.e. by working with the intelligence assessment units housed within other departments and agencies) and internationally with Five Eyes partners. The Assistant Secretary of

IAS participates in the Heads of Assessment forum with his or her Five Eyes counterparts, which meets annually. Informally, IAS officials from the working to senior levels are in daily contact with their Five Eyes counterparts.

1.2   Security and Intelligence Secretariat:

[5]   Nabih Eldebs is Assistant Secretary, S&I. He has held this role since December 2023. As Assistant Secretary, he is responsible for overseeing all four branches of the S&I Secretariat: Operations ("**OPS**"), Strategic Policy and Planning ("**SPP**"), the Review Coordination Unit ("**RCU**"), and the Security Operations Directorate ("**SECOPS**"), each of which has its own Director. In addition, S&I houses a Security Centre of Excellence which provides policy advice on national security issues. The Assistant Secretary of S&I participates in the Intelligence Policy Forum ("**IPF**"), a forum that performs the central security and intelligence coordination function within the Five Eyes, addressing strategic, policy and issues management matters within the Five Eyes intelligence community.

[6]   Michael MacDonald was interviewed in his capacity as former Assistant Secretary, S&I. He held this role from May 2020 to June 2023. He now serves as a Senior Assistant Deputy Minister at the Treasury Board of Canada Secretariat, and formerly served as the interim Acting NSIA from July 16, 2021 to August 3, 2021 while David Morrison [the Acting NSIA at that time] was on temporary leave.

[7]   Bridget Walshe was appointed the Director of Operations, S&I, in June 2022. Before assuming this role, she worked at CSE in foreign intelligence and cyber security. In her role as Director of Operations, Ms. Walshe handles operational issues related to security and intelligence, convenes the national security community, and ensures a quick response to pressing issues, advising the Prime Minister's Office as appropriate. She noted that S&I handles a broad range of issues, including, for example, foreign interference, cyber threats, counter terrorism, Ministerial security, and the national security dimensions of financial crime. S&I works closely with the Security and Intelligence Threats to Election Task Force ("**SITE TF**"). The role of OPS is not limited to consuming intelligence, but also involves working with the intelligence community to

determine who needs to know the intelligence to ensure it is addressed, and performing a "challenge function" on the options and strategic issues that arise in relation to that intelligence. Ms. Walshe's role also touches on policy issues, as OPS performs a challenge function on operational policy (e.g. the operational decision-making process, operational gaps, etc.). Ms. Walshe served as Acting Assistant Secretary of S&I from October – November 2023.

[8]   Adelle Ferguson is the Director of Strategic Policy & Planning ("**SPP**") at S&I. She has been in this position since September 2022. This unit handles strategic policy issues including economic security, violent extremism, foreign interference, and intelligence priorities, among other files. As Director SPP, Ms. Ferguson is responsible for providing advice on those policy issues for the Prime Minister and senior PCO officials; coordinating the S&I community in advancing the development of strategic policy initiatives; performing PCO's challenge function on those initiatives; and supporting the DC-NSIA, DNSIA and Assistant Secretary, S&I in their participation in specific interdepartmental committees, including the Deputy Minister's Committee on National Security and the Assistant Deputy Ministers' National Security Policy Committee. She is also the lead for S&I on matters related to international engagement.

[9]   Marie-Hélène Chayer was interviewed in her capacity as former Acting Assistant Secretary, S&I. She held this role from June to October 2023. Before this role, she headed PCO's Task Force on Foreign Interference (from January 2023). She currently serves as Assistant Secretary to the Cabinet, National Security Council ("**NSC**"). In this role, she provides support to the Prime Minister and NSC, as well as the Cabinet Committee on Global Affairs and Public Security ("**GPS**") and the national security-related meetings of the Incident Response Group ("**IRG**").

2. Threat Landscape: Then and Now

2.1   National Security Outlook

[10]   Mr. Green described foreign interference ("**FI**") as historic. He noted that attention on this issue picked up in 2016, when allegations of Russian interference in the United

States presidential election prompted discussions within the Five Eyes community. PCO-IAS produces a number of intelligence assessment products including a "National Security Outlook", a joint product created with conjunction with other departments and agencies that sets out, in a placemat format, the strategic national security landscape at the time of publication and for the year ahead. He confirmed that in recent years, FI issues have always been part of this document, though FI is now blending into other issues, such as cyber security or emerging technologies.

[11]   Mr. Green explained that the People's Republic of China ("**PRC**") and India are the two biggest threat actors from an FI perspective. The National Security Outlook for 2024 reflects this assessment.

[12]   In response to a specific question about how FI has evolved since 2018, Mr. Green indicated that it is difficult to give a weighted measure to the most pressing threats to Canada's national security. Generally speaking, FI is becoming bigger, more sophisticated, and more difficult to detect [His comment referred to FI generally and was not limited to FI in democratic processes]. He noted that FI continues to evolve, as foreign threat actors routinely stop certain activities and re-start others, based on Government of Canada's detection and response. He also noted that FI is targeted at all levels of government, including federal, provincial/territorial, and municipal, though he noted that responding to FI at the subnational level is difficult given the limits of the federal government's jurisdiction. Mr. Green added that other countries are using a diverse toolkit to conduct FI activities [not limited to FI in democratic processes], including cyber tactics, economic coercion, and military coercion. There is no bright line distinguishing FI from foreign influence, and some activities fall into a "grey zone" between the two.

2.2   Artificial Intelligence

[13]   Commission Counsel directed the witnesses to an infographic entitled "Artificial Intelligence (AI) Risk Inventory".[1] Mr. Green explained this document received

---

[1]   CAN032039.

significant interest from recipients, and reflected PCO-IAS's judgement that artificial intelligence will cause major disruption in multiple areas, for example, in labour markets. This placemat represented a first effort to set out the AI landscape from a threat lens, including the potential social and economic disruptions. Mr. Green noted that the PRC and European Union are taking steps to regulate this technology, and the US has issued executive guidance to the private sector in this area.

[14] Mr. Green noted that the technology was moving quickly, and in his personal view, it would be necessary to work with the private sector and other non-traditional partners to confront the challenge.

[15] Mr. Eldebs clarified that Canada is ahead of the international community on AI, noting that Canada has the three top AI researchers in the world. Innovation, Science and Economic Development Canada and CSE have been leading an immense effort within the Five Eyes and the broader international community to champion the effort to confront AI challenges.

[16] Mr. Eldebs added that AI should not be viewed only as a threat but also as an opportunity. Ms. Chayer agreed, adding that AI can also be used as a tool to bolster Canada's national security capabilities.

[17] Ms. Ducharme noted that the AI placemat was dated April 2023 and represents a snapshot in time. She explained that the government has done a significant amount of work on AI since then, and that work is ongoing. For example, IAS conducted an intensive "red-teaming" exercise with Government of Canada intelligence and policy colleagues and Elections Canada and Leaders' Debate Commission staff to examine how AI can be used to strengthen or threaten election security. The exercise used a forward-looking lens, examining not only what the community has actually seen happen but also looking at how AI may be misused in the future. The goal was to identify specific threats while also building resilience to those threats. A report based on this exercise is in the process of being finalized and has already been shared with the Five Eyes for feedback and to develop and exchange best practices. Ms. Walshe added that the community is taking the great work done by the red-team workshop and using it to inform operations, for example, to identify and take down deep-fakes.

2.3   Changes in the Work of S&I and IAS

[18]   The panel was asked how the work of S&I and IAS has evolved, as the threat evolved. Mr. Green said that over the past 9 years, IAS did a lot of assessments focused on foreign, geopolitical issues. Over time, national security issues have become more integrated, leading to a more functional rather than topical approach, and collaboration between foreign and domestic assessment groups has become more common place. For example, Mr. Green explained that he created an emerging tech group within IAS that looks not only at AI but also at emerging issues in biotechnology. Mr. Green noted that there has been significant uptake in the functional approach to intelligence coordination across government as Deputy Ministers appreciate that many issues touch on the functions of multiple departments.

[19]   In response to the question of how the work of S&I has evolved, Mr. Eldebs noted that when he came into his current role, S&I was a well-oiled machine, and that the flow of information to the NSIA and PM works well, thanks to the PCO team. He explained that PCO S&I tries to integrate and liaise with other organizations, like Public Safety, as much as possible. He noted that even though intelligence develops faster than policy, he believes the two are connected and has been working to ensure that intelligence feeds policy development.

[20]   Building on Mr. Eldebs' response about how the work has changed, Ms. Chayer said that the speed at which PCO can activate governance committees at the director general, assistant deputy minister, and deputy minister levels in relation to intelligence [not limited to FI] has evolved. For example, she noted that DMCIR can be stood up rapidly even on an *ad hoc* basis when required.

[21]   It was suggested to the witnesses that a 2024 NSIRA report found that there was a lack of understanding of the threat of FI or the gravity of the threat among senior government officials. Mr. Eldebs disagreed with that assessment. He described the line between foreign influence and FI as "small" and "fuzzy", and explained that, determining where one ends and the other begins requires debate. He noted that intelligence is comprised of building blocks, and the picture that forms is not only subject to interpretation but changes over time. When looking at a piece of intelligence in isolation, it is easy for

consumers of intelligence and review bodies (e.g. NSIRA, NSICOP) to come to different views. That is why there is room for disagreement about how to characterize some activities. Differing views often help focus the issue.

[22] Mr. Macdonald made five observations about the work of S&I during his tenure. First, he commended the relationship between S&I and Elections Canada, noting both his own positive relationship with his counterpart, and also the impressive cooperation between Ms. Walshe and the OPS team and their counterparts at Elections Canada. Second, he noted investments that S&I had made in its relationship with the Sergeant-At-Arms, the Parliamentary Protective Service and the Chief of Senate Security. Third, he noted a maturing of the process for developing the intelligence priorities and the ability to measure the performance of the intelligence community against those priorities using data. Fourth, he noted the creation of the Assistant Deputy Minister Tactical Committee ("**ADM Tactical**"), a committee that deals with cutting edge and operational issues-management, and supports the government's ability to generate options and coordinate responses. Fifth, he noted that PCO/SECOPs has improved the quality and depth of their briefings to new ministers and parliamentarians, particularly on issues related to physical and cyber security.

[23] Mr. Green described the fast-paced growth of civil society organizations aimed at combatting mis- and disinformation, such as Citizen Lab. He said that partnerships with this type of organization will be important as Canada continues to combat FI.

[24] Ms. Walshe responded to the question about the evolution of the work of S&I through an operational lens. She agreed with Mr. MacDonald that a significant amount of work has been done in conjunction with Elections Canada, but noted that efforts have been far broader than that. She described the work done to implement enhanced monitoring by SITE TF during by-elections. She noted that the SITE TF process for by-elections has become well institutionalized over the last year or so. She also noted that a significant amount of work had been done to support committees, describing the work she has done with PS to institutionalize the workflow of both ADM Tactical and DMCIR to ensure that rapid support for these committees is a matter of practice, and not dependent on the composition of the committees.

3. Intelligence Collection, Distribution, Sharing and Action-On

3.1   Intelligence Priorities

[25]   Mr. Eldebs described the Canadian Intelligence Priorities as a high level guide for the intelligence community. Intelligence Priorities are set every two years, by Cabinet. The process for developing these Priorities is intensive and is coordinated by Ms. Ferguson and her team. It involves working with the entire intelligence community. They are based on the government's intelligence needs, taking into consideration what intelligence departments and agencies have the ability to collect, and what Canada can expect to receive from allies. Every year, S&I leads a '360 degree review' of the Priorities and the requirements. As part of this review it receives reports from the security and intelligence community on their respective operationalization of the Priorities and provides an annual update to Cabinet.

[26]   Ms. Ferguson explained that there is a systematic process and well-established structure for developing intelligence priorities, which operates on a two-year cycle and engages intelligence committees at the Director General, ADM and DM levels. The first stage involves a proactive outreach across the government intelligence community, made up of both intelligence consumers and collectors. To assist this outreach, there is an effort to identify Government policy priorities, both current and anticipated over a 2 year horizon, as reflected, for example, in Ministers' mandate letters, departmental priorities, or previous government commitments. This process is iterative. Outreach to collectors helps clarify what is and is not possible when it comes to intelligence collection, and outreach to consumers helps to clarify what sort of intelligence is needed. SPP then works with the community to align the two. Once the process is complete, a list of priorities is formed. Ms. Ferguson explained the priorities are deliberately not ranked in order to enable the government to focus and allocate resources as needed, leaving flexibility to adjust if necessary (e.g. if there is another incident like 9-11, one would expect a shift to place a greater emphasis on intelligence related to terrorism).

[27] Underneath the intelligence priorities are intelligence requirements, which are more granular. In consultation with the intelligence community, intelligence requirements are tiered into four different priority levels to manage resources. Ms. Ferguson described this as an evergreen process. If a new event arises, the community can reconvene and adjust.

[28] Mr. Green said that IAS evaluates all of its intelligence products with reference to the Intelligence Priorities.

[29] Mr. Eldebs explained that within the Five Eyes, every country sets its own priorities. However, given that the Five Eyes face similar threats and issues, the intelligence priorities of the Five Eyes naturally align. He described ongoing engagement amongst the Five Eyes to discuss intelligence priorities and efforts to avoid duplication. Each member may have an area of focus, based on their strengths. Mr. Eldebs stated that this coordination currently takes place and works very well.

[30] Mr. MacDonald added that when he chaired the IPF, coordinating the Five Eyes' efforts was part of the work-plan, and all of the partners had very similar priorities.

[31] Ms. Chayer added that collaboration with Five Eyes allies is frequent, and happens at both the working levels and senior levels of government. She noted that when she was the head of assessments at DND and when she was in charge of the Integrated Terrorism Assessment Centre within CSIS, she would routinely pick up the phone to speak with her Five Eyes counterparts. She described the Five Eyes philosophy as working "around the sun"—as each partner keeps watch when the others cannot. She agreed with her colleagues that cooperation with the Five Eyes when it comes to the collection, assessment and dissemination of intelligence is constant and ongoing.

[32] Ms. Ducharme noted, as an example of this collaboration, a paper that the IPF tasked the Heads of Assessment to prepare on a "hard target subject" (i.e. a topic for which gathering intelligence is challenging) where Canada is taking the lead. The Five Eyes have working groups devoted to the subject, which was discussed at a Five Eyes meeting in New Zealand in the week after this interview took place.

3.2   Intelligence Circulation and Tracking

[33]   Mr. Green explained that IAS publishes a variety of intelligence assessment products, each with a different angle. For example, IAS puts out a Daily Foreign Intelligence Brief ("**DFIB**") that reflects three to four important intelligence items gleaned from raw intelligence. The dissemination of DFIBs is widespread. IAS also circulates the Prime Minister's Weekly Intelligence Brief ("**PMWIB**"), which may contain highlights from the DFIBs, or it may be focused on intelligence related to upcoming events. The dissemination of other products varies. He noted that IAS has colleagues at CSE and Canadian Forces Intelligence Command who also receive products from IAS as they are often consulted on them. IAS also provides oral briefings to the Prime Minister's Office ("**PMO**"). Much of this intelligence has the security marking "Canadian Eyes Only".

[34]   Ms. Ducharme explained that all IAS products written for community consumption are posted on Canada's Top Secret Network, the IAS website, and [systems managed by CSE] for use by Client Relations Officers [CSE employees housed in other government departments, charged with the responsibility of communicated CSE intelligence to officials in those departments]. She noted that there are always improvements to be made to the dissemination process. In addition to making products available in these systems, IAS uses a "push" system (i.e. sends email links) to specific points of contact, depending on the product. IAS may also respond to requests for information from its clients. For example, if a senior official is traveling to the G7, or to a foreign country, efforts are made to align the products IAS sends with intelligence relevant to that country or those agenda topics. Ms. Chayer echoed that there is an effort within the intelligence community to track what intelligence is briefed up and tailor intelligence packages to the needs of clients.

[35]   Ms. Ducharme noted that there has also been a concerted effort to write IAS products at a lower classification level so that they can reach a wider audience.

3.3   Distribution of Specific CSIS Product

[36]   Commission Counsel directed the witnesses to a classified email chain. [This is an email chain that indicates IAS was not on the distribution list for a Canadian Security Intelligence Service ("**CSIS**") product, which meant that it was not initially incorporated into a draft IAS product. The email describes this as a "broader dissemination issue that [IAS] hope[s] to resolve in the future." IAS was ultimately able to receive and review the assessment.]

[37]   Ms. Ducharme explained that CSIS would be better placed to speak to its own dissemination processes, but in the past, certain CSIS operational reporting was addressed to specific positions or names. Ms. Ducharme explained that IAS assessment products have historically focused on foreign strategic pieces, whereas S&I is the unit that focuses on domestic and operational intelligence [the CSIS product in question was operational and domestic].

[38]   Ms. Ducharme explained that her comment in the email chain was a reference to work being done by all originating government departments to review their dissemination lists on an ongoing basis, particularly in light of the trend toward assessment pieces that bring together the foreign and domestic aspects of an issue, as well as providing operational examples with the strategic context. After the interview, the witnesses noted that this trend is not unique to Canada but reflects a change in approach across the Five Eyes.

3.4   NSIRA Report and the Grey Area

[39]   Commission Counsel suggested to the panel that the NSIRA report[2] raises a question about how to define FI in relation to legitimate diplomatic activity. Commission Counsel noted that different departments and agencies may have different perspectives (e.g. GAC may have a different view than CSIS) and asked the panel to speak to it from the perspective of PCO's convening and coordination function.

---

[2] NSIRA, "Review of the dissemination of intelligence on People's Republic of China political foreign interference, 2018–2023" (2024).

[40] Mr. Green commented that each department and agency is going to look at the issue from the perspective of their own mandate. For example, CSIS operates under the *CSIS Act*, which authorizes them to look at threats to the security of Canada, leading them to view information through that lens. Mr. Green noted that while IAS has attempted to distinguish between foreign influence and foreign interference in an assessment product, it is difficult to distinguish the two concepts completely because there is a significant grey area. The issue, and our toolkit, needs to be looked at holistically.

[41] Ms. Walshe agreed that there is a grey area. She added that each department and agency looking at the issue from their own lens is the reason for PCO's convening function—the purpose is to bring the community together (e.g. at ADM Tactical and DMCIR) to have a healthy discussion about a particular activity, to determine where it fits on the spectrum. She reiterated that the system is in place for this to happen regularly and rapidly.

[42] Mr. MacDonald echoed that most like-minded countries have to grapple with this grey area. By way of a metaphor, he noted how different people may have different perspectives on the line between passionate expression and aggression, teasing and bullying, or what constitutes a violation of personal space. Distinguishing between these concepts requires reliance on contextual clues, which are situation-dependent.

4. Outreach to Other Entities

4.1   Outreach to Parliamentarians

[43] Commission Counsel referred the witnesses to a CAN043176. [This is a point-in-time document describing Canada's counter-foreign interference approach, and, among other things, summarizes work being done by departments and agencies to notify appropriate ministers and officials about any intelligence regarding threats to MPs or their families.] The witnesses were asked what safeguards were in place to ensure the information was communicated to affected MPs.

[44] Mr. Eldebs explained that ADM Tactical and DMCIR are the committees set up to address intelligence response and that there is a robust process in place for sharing

intelligence with key partners and developing options for response [not limited to intelligence relating to Parliamentarians]. Mr. Eldebs observed that the process is working very well, and that ADM Tactical can be called on an hour's notice. ADM Tactical is typically the precursor for DMCIR. S&I, as the secretariat for DMCIR, can also call a DM meeting on short notice when needed. Mr. Eldebs noted that the system can be agile and geared for rapidity.

[45] Ms. Chayer noted that the document referenced is a draft, issued by the Minister of Public Safety to CSIS, and that she is not sure when it was created. She said that a protocol has been developed setting out how to share information about threats to Parliamentarians, and that CSIS and PS could speak to that. She noted that both ADM Tactical and DMCIR have been written into the system outlined by the protocol.

[46] The witnesses were taken to a classified document and asked whether the framework discussed therein had actually been implemented. Mr. Eldebs confirmed that the Ministerial Directive discussed in the email had been implemented, and that it was an agile process. He observed that CSIS can flag intelligence for ADM Tactical, and that S&I also receives this intelligence as a matter of course, and can proactively add it to the agenda as well.

4.2   Outreach to Political Parties

[47] The witnesses were asked about a concern expressed by certain political party representatives regarding the level of information they were provided in FI briefings in the past. Mr. Eldebs said that political party representatives do not always have the requisite security clearance to receive a classified or top secret briefing. PCO has offered to sponsor clearances to political parties more than once, but not all parties have taken them up on the offer. At present, there have also been briefings before every by-election, but there has been little interest from political parties in participating. In addition, Mr. Eldebs noted that the NSIA recently sent letters to political party leaders offering them security clearances so that they can obtain regular classified briefings. PCO continues to engage with political parties.

[48] Ms. Walshe said that S&I tries to make security briefings as relevant possible, and that they worked to develop processes to provide briefings and enhanced monitoring for by-elections in a fashion similar to the work done during GE43 and 44. S&I has made it clear that these briefings are offered systematically to all parties, and has sought feedback on the briefings that have been delivered. She noted that SITE TF delivers the briefings, though S&I works closely with SITE TF on them.

[49] Mr. Eldebs does not know why certain political parties have not taken the government up on its offer of clearances or briefings. However, all Parliamentarians have received an FI briefing quite recently, and that S&I hopes to conduct more briefings in the future.

4.3   Outreach to Provinces and Territories

[50] Mr. Eldebs explained that in past years, PS co-led a national security table with the provinces and territories on national security issues. This table stopped meeting [including due to COVID], but recently, S&I and PS have worked to revive it. The table met recently in 2024. S&I has also engaged with the Intergovernmental Affairs Secretariat within PCO to ask provinces to identify appropriate counterparts with whom to engage on national security issues.

[51] Mr. Eldebs observed that there are different levels of engagement across provinces and some provinces have more well-developed structures in place for this engagement. Some provinces have well-established positions focusing on national security issues, others do not. Some have officials with clearances, others do not. The Clerk of the Privy Council is engaging with his provincial and territorial counterparts to encourage greater engagement, and offer security clearances so that they can engage at a Secret or Top Secret level. This work is ongoing. The Clerk of PCO has a further meeting with his counterparts next month to move this discussion forward. As part of the Clerk's upcoming meeting, Mr. Eldebs is coordinating a briefing to provincial/territorial officials on foreign interference and cyber security.

5. National Security Committees and Other Governance

5.1   Proposals to Revise National Security Governance Structures

[52]   Commission Counsel directed the witnesses CAN037056. [This document details a proposal to streamline Canada's National Security and Intelligence governance structure. It states that Canada's current NSI governance structure is not optimally or efficiently organized, and presents options for a renewed governance structure.]

[53]   Mr. Eldebs noted that discussions on the renewed governance structure were ongoing. The "Five Committee Option", set out on page seven of the document, is the model that is currently being closely considered, but emphasized that no decision has yet been made.

[54]   Ms. Ferguson cautioned that the document is an early draft, and the proposal has since evolved. She noted that one of the features of the renewed governance structure that is being considered is the creation of a centralized secretariat function at PCO that would support all of the DM Committees. She noted that this would involve taking some of the functions currently provided by other departments acting as secretariats (i.e. agenda management, scheduling, organizing meeting materials, etc.), and centralizing them in one Secretariat located in PCO, strengthening coordination.

[55]   Commission Counsel then directed the witnesses to a classified document. [This is an earlier document setting out a proposal to reform the Deputy Minister Intelligence Assessment Committee ("**DMIA**").] Ms. Ferguson explained that if the proposal for the renewed governance structure was approved, it would supersede this proposal.

5.2   Deputy Minister's Intelligence Committee ("DMIC")

[56]   Commission Counsel directed the witnesses to a classified email chain. [This is an email chain that says DMIC did not meet from June 2021 to January 2022, and states an impression that the committee had turned into "largely a paper-editing exercise." It also states that as of late 2022, the NSIA tasked IAS with updating the DMIC Terms of Reference.] Commission Counsel ask why DMIC had not met for nearly two years, and why work was being done to update its Terms of Reference.

[57] Mr. Eldebs explained, by way of background, that there are numerous DM-level committees. He explained that when a new issue emerged, a committee would be stood up to address it. Sometimes, these committees would evolve and subsume the work previously done by other committees, but committees that had become moot were rarely formally disbanded. This is one of the reasons for the larger governance review. In this case, both DMCIR and the Deputy Ministers' Operational Committee ("**DMOC**") had overtaken the work previously done by DMIC. Ms. Chayer said that even though DMIC was not meeting, relevant intelligence was still discussed in other committees and intelligence assessments distributed to clients.

[58] Mr. MacDonald provided background context for the two years when DMIC did not meet. First, he pointed out that this was in the middle of COVID, and so classified meetings in general were logistically challenging and less frequent. Second, he noted that the acting NSIA at the time, David Morrison, who was also the Foreign and Defence Policy Advisor to the Prime Minister, was managing a number of pressing operational issues, including the arbitrary detention of the two Michaels in China, the evacuation of Kabul, and growing intelligence related to the impending invasion of Ukraine. This context may help explain why the focus shifted to those committees with an operational mandate, like DMOC.

5.3   Deputy Ministers' Committee on Intelligence Response ("DMCIR")

[59] Mr. Eldebs explained that at the beginning of his tenure, DMCIR met in direct response to intelligence as it arose. Now, meetings are scheduled in advance and supported by a formal, rigorous process. Intelligence that is discussed at DMCIR can be flagged by its members, including intelligence agencies, or S&I. Once an agency or S&I flags a piece of intelligence for discussion, it is discussed at ADM Tactical for a discussion about whether a response is required and options for a response. This work flows up to DMCIR who evaluates these ideas and options, though DMCIR can also be called *ad hoc*. Ms. Chayer underscored that DMCIR is not just for thinking about where intelligence ought to go, but also what, if any, operational response is required and who should act on it. The DMs who participate in DMCIR have the authority to act within their

departments' mandates. The purpose of meeting is to share perspectives and ensure a coordinated response.

[60]   Ms. Walshe explained that S&I is the secretariat for DMCIR. In that capacity, S&I not only keeps an eye on the intelligence that is coming in, it also tracks and follows-up with departments on actions coming out of DMCIR that are being executed by the departments. She explained that ADM Tactical is often used for this purpose.

[61]   Commission Counsel directed the witnesses to CAN025982, an undated document of unknown authorship called "GAC Response Timelines and Activities – Summer / Autumn 2023", which alleges that a PRC-led disinformation campaign against Canadian MPs, called "Spamouflage", struggled to get on the agenda at DMCIR, and CAN025988 an undated document of unknown authorship entitled "Lessons Learned Spamouflage," which notes an "[o]verall frustration regarding *DMSIR* [sic] and the fact that it is lagging on the response part".

[62]   Mr. Eldebs did not recognize either document. He noted that, he has been impressed with the speed of the DMCIR process and the effectiveness of having all of the DMs around the table, the result of considerable work that was done to set up a rapid system. He noted that in the six months he has been at S&I, Mr. Eldebs has not heard any complaint from any department regarding any delays in the DMCIR process. His experience contradicts the assessment contained in this document.

[63]   Ms. Ducharme explained that IAS was actually the secretariat at the time of the Spamouflage incident and she could speak with direct knowledge on this issue. She stated that there is a disconnect between what the author of the document is describing and what actually occurred. She recalled that the Spamouflage issue was flagged immediately, the issue was added to the agenda, and materials were put together expeditiously. She explained that due to exigent circumstances, DMCIR was not able to meet that same week, and so it met the following week. She suggested that the unknown author may not have been aware of those exigent circumstances and therefore misunderstood the situation. In her view, the document was written by someone who did not know what had actually happened.

[64] Bridget Walshe, who was also personally involved, confirmed that the Spamouflage issue was discussed and actioned expeditiously.

5.4   Task Force on Foreign Interference

[65] Ms. Chayer indicated that PCO's Task Force on FI was a short-term initiative meant to add surge capacity within PCO to address FI. She explained that she prepared the original draft Terms of Reference for discussion. The original concept was to utilize the additional capacity to help coordinate the government response to FI-related matters. However, after further discussion with key partners involved in the file including at PS (which ultimately became the FI Coordinator role), the Task Force was redirected to assist in coordinating policy efforts in the FI space. For example, they provided support in the preparation of the Charette-Leblanc report.[3] The Task Force supported work that eventually turned into Bill C-70 [An Act respecting countering foreign interference, which received royal assent on June 20, 2024]. The Task Force was not a committee or secretariat. It was comprised of Ms. Chayer and three colleagues who together provided additional capacity to PCO.

5.5   National Security Council

[66] Ms. Chayer was asked to explain the remit of the NSC and how its remit would change following the governance renewal process discussed earlier. Ms. Chayer explained that the NSC [a new Cabinet committee chaired by the Prime Minister, which serves as a forum for strategic decision-making and for sharing analysis of intelligence in its strategic context] is not part of the governance renewal document discussed earlier. It is a Cabinet committee, not a DM committee. The NSC looks at strategic national security issues and increases awareness on these issues writ large. Ms. Chayer explained that the NSC does not necessarily look at tactical or operational intelligence issues, whether related to FI or otherwise.

---

[3] Government of Canada, "Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions" (2023).

5.6 Elections Canada

[67] Mr. Eldebs advised that the Election Security Coordinating Committee ("**ESCC**") [this committee, co-chaired by S&I and Elections Canada, provides direction for ensuring interagency collaboration, coordination and system preparedness as it relates to electoral security] meets regularly. He added that ESCC is a useful body for dealing with elections-related issues. The cadence of meetings increases in the lead up to and during elections.

6. Policy Initiatives, Gaps, and Solutions

6.1 Bill C-70 and Other Legislative Changes

[68] Mr. Eldebs said that Bill C-70 is the largest piece of legislation addressing FI since Bill C-59 [a former bill, tabled in 2017, that enacted a stand-alone *Communications Security Establishment Act*, revised some of CSIS's powers, and created the National Security and Intelligence Review Agency, among other things]. Mr. Eldebs said that both were very important. Mr. Eldebs emphasized that FI is a complex threat and ever-changing. He explained that the *CSIS Act* was written for an analog world and that changes to the legislation were necessary to deal with the challenges of a digital world. He explained that policy development in the national security community has to take into account Canadian values, noting that the *Privacy Act*, and the *Canadian Charter of Rights and Freedom* are of critical importance. He posited, however, that our notion of privacy has changed even in the last ten years and needs to evolve as our world becomes increasingly digital.

6.2 Declassification Policy

[69] Commission Counsel directed the witnesses to CAN034284. This isa slide deck entitled "Declassifying Intelligence", which sets out considerations and a possible framework for a declassification protocol.

[70] Mr. Eldebs explained that this document was not related to the Canada's ability to detect, deter and counter FI. He explained that this slide deck is discussing a

declassification policy similar to that of the United States, where classified documents undergo an automatic review after a specified period of time (e.g. in the U.S. it is 25 years) to determine whether the documents need to remain classified or whether they can be declassified either fully or an a redacted format. The purpose of a declassification strategy, which is a resource-intensive exercise, is to ease the government's burden in responding to ATIP requests for historical documents and to increase transparency.

[71]   Mr. Eldebs distinguished declassification [the process by which historical documents undergo a review to determine whether they need to remain classified] from sanitization [the process by which a document with a higher security marking is edited to be suitable for circulation with a lower security marking or for public release]. He emphasized that sanitization of current intelligence, so that it can be shared with the public, used in briefings, etc., is not the subject of this presentation.

[72]   Mr. Eldebs was asked about what appeared to be an earlier version of the same presentation [CAN026308] which states that the current reality "creates tensions in international relationships as responding to declassification requests can be time consuming & disclosure may not be possible." Mr. Eldebs said, again, that this was talking about requests to declassify historical documents, not requests to sanitize or use current allied intelligence. Mr. Eldebs said that there is no tension with Five Eyes partners when it comes to declassification or sanitization. He explained that there are well-established processes in place to sanitize or use allied intelligence. These are mutual processes, as Five Eyes partners are very cognizant of the need to protect each other's equities and sources. The sources and methods of the Canadian security agencies and those of our allies are achieved through a lot of hard work and can include years of technical effort or, alternatively, work to develop human sources. The work to develop sources and methods is expensive and hard fought. These sources and methods are sensitive and could disappear very easily if intelligence is not handled responsibly. Any slip that jeopardizes the sources and methods of our Five Eyes partners could cause them to rethink how much intelligence they want to share with Canada in the future. That is not a tension; it is a mutual interest in protecting each other's equities.

[73] Mr. Eldebs explained that the public narrative and the push to release increasingly more classified intelligence is sometimes unfortunate because it does not take into account these delicate realities. He commented that Canada's intelligence community actually produces a significant amount of write-to-release information for public consumption. In his view the intelligence community has been quite transparent, going so far as to put out public products that call out specific countries on FI. The public will always want to know more. When making intelligence more accessible, he explained, decision-makers must always balance the future of intelligence collection and the safety of human sources, against public interest and the value of transparency.

[74] Ms. Chayer added that there are ongoing efforts to increase transparency but that intelligence officials in Canada are trained to protect information, including sources. The improper release of classified information could jeopardize the lives of human sources.

[75] Mr. Green added that IAS deals with a large volume of ATIP requests. The trend in the national security community is moving toward greater disclosure and greater transparency by preparing more products at an unclassified or lower level of classification. He agreed that there does exist a very real danger of jeopardizing the safety, and even the lives, of human sources. He noted that Canada is a net beneficiary when it comes to the Five Eyes alliance because we receive more intelligence than we produce, and we would not want to jeopardize that. Mr. Green noted that some Canadian intelligence products are classified as Canadian Eyes Only, which means that they are not shared with partners. He suggested there are opportunities to better leverage open source intelligence ("**OSINT**") to help prepare intelligence that can be shared more widely.

[76] Ms. Ducharme stated that there were ongoing discussions between IAS and its clients about preparing more products at the unclassified level that can be more widely disseminated. Ms. Chayer concurred, noting that CSIS and CSE both publish reports on their websites and suggested that the Commission may wish to speak to those organizations, as the collectors of intelligence, about their efforts to increase awareness of FI.

6.3   Open Source Intelligence Collection

[77]   The panel was asked whether the Government of Canada has any formal relationships with private sector or civil society organizations working on OSINT. Mr. Green explained that different departments and agencies are using OSINT in different ways and have different partners. He noted that during his time, IAS did not have any formal partnerships. IAS has used some open source data mining tools on a small-scale to supplement the work of analysts, and added that these types of tools will become "huge disruptors" as they grow in sophistication. He noted that IAS has had discussions with allies about what they are doing in this space through the Heads of Assessment forum and said that in his view, IAS should continue to pursue this space.

[78]   Ms. Ducharme noted that IAS is currently leading an inter-departmental working group of experts on OSINT. The working group meets on a regular basis to develop standards and best practices for the use of OSINT tools and analysis of OSINT data.

[79]   Mr. Eldebs drew a distinction between OSINT and publicly available information and cautioned that just because something is open-source (i.e. not classified or obtained covertly), does not mean it is meant to be public, and there are different legal and ethical considerations that have to be kept in mind before adopting a particular OSINT tool or accessing OSINT data. For example, if a threat actor steals information and puts it on the dark web, that is considered OSINT. But that does not mean that anyone should be accessing and using that information. He explained that new OSINT tools need to be carefully evaluated, and there are ongoing discussions around striking the right balance.

[80]   Mr. Green concurred, noting that there are legal and reputational considerations to the use of OSINT tools. He added that even storing large OSINT datasets raises questions about the purpose for which the information is being maintained, and the vulnerabilities that are being created (e.g. to cyber-attacks). He indicated that simply collecting as much OSINT as possible could pose as much of an FI vulnerability as it would be a tool to combat it.

6.4 Communication Strategy regarding Mis-Disinformation

[81] The panel was asked about whether PCO-Comms (a separate secretariat within PCO) had a communications strategy to combat mis- and disinformation. Mr. Eldebs said that PCO-DI is currently working with PCO-Comms and may be able to provide more information on the communications strategy.

7. Questions from the Attorney General of Canada

7.1   Distinction Between Intelligence from IAS and S&I

[82] IAS was asked by Commission Counsel about its role as a conduit of intelligence to the Prime Minister. The Attorney General of Canada asked the witnesses to explain the difference between the types of intelligence products that IAS produces and disseminates, and the role of S&I in flagging intelligence. Ms. Ducharme explained that IAS produces broad, strategic assessments. These assessments are high-level and forward-looking, targeting a horizon of between 6 months and 2 years ahead, depending on the product. By contrast, Ms. Walshe explained that S&I receives intelligence as a client of intelligence agencies. The intelligence that they receive and flag for senior officials is operational or tactical in nature (e.g., a kidnapping of Canadians). She explained that S&I has a role in flagging operational intelligence to PMO, and that the process for disseminating this intelligence is tracked and well-recorded.

[83] Ms. Ducharme commented that IAS describes the forest while S&I addresses the trees. Mr. Green explained that the assessments IAS provides can enhance the narrative of a single piece of intelligence, and that the two work together.

7.2   Governance Renewal Process

[84] The Attorney General of Canada referred the witnesses back to CAN037056, a document which details a proposal to streamline Canada's National Security and Intelligence governance structure and asked witnesses to comment on the impetus for the renewal process.

[85] Ms. Ferguson said that the impetus for this proposal came from the fact that there had been a proliferation of committees and that the structure had not been reviewed for some time. There was a broader sense that it was time to revisit this structure, to determine whether the current structure was optimal.

[86] Mr. MacDonald said that the committees worked well during his time as Assistant Secretariat, S&I. The strength of the chairs is important, and he relied on the coordination and discussion within committees to help him fulfill his role. He noted that he found co-chairing committees helpful, as it allows for greater diversity of perspective.

[87] Ms. Chayer commented that it is healthy and a sign of maturity in the system to take a look at governance issues periodically. The national security landscape is always evolving, and so it is natural when things change to take a look at how government systems might also evolve and improve.