Interview Summary: David Vigneault, Michelle Tessier, Tricia Geddes (Canadian Security Intelligence Service) and Marie-Hélène Chayer (Integrated Terrorism Assessment Center)

Background

Senior officials from the Canadian Security Intelligence Service and the Integrated Terrorism Assessment Centre were interviewed in a panel format by Shantona Chaudhury, Gordon Cameron, Yves Côté and Nusra Khan on August 29, 2022. Questions relating to this summary should be directed to Ms. Khan.

The interview was held in a Top-Secret environment and included reference to sensitive or potentially injurious information under section 38 of the *Canada Evidence Act*. This summary has been drafted in a manner that removes or summarizes all references to such information so that the summary can be disclosed publicly. Publicly disclosable versions of the documents cited in this summary are expected to be available to the Parties shortly.

This summary should be read in conjunction with the unclassified Institutional Report prepared by CSIS.

This preamble and the text contained in square brackets are explanatory notes provided by Commission Counsel for the assistance of the reader.

The **Canadian Security Intelligence Service (CSIS)** is a civilian security intelligence service. The core mandate of CSIS is to investigate threats to the security of Canada and advise the Government of Canada on such threats. The *Canadian Security Intelligence Act (CSIS Act*) identifies the specific activities that the Service may investigate as well as the threshold that must be met for CSIS to engage in investigative activities and take threat reduction measures.

The **Integrated Terrorism Assessment Center (ITAC)** was created in 2005 and is collocated with CSIS Headquarters. It operates under the provisions and authorities of the *CSIS Act*. ITAC does not collect intelligence. It is an assessment body that analyzes terrorism-related intelligence and independently produces threat assessments to support government and law enforcement decision-making. In producing its threat assessments, ITAC relies on intelligence collected by domestic and international partners, including CSIS, as well as open source information.

David Vigneault was appointed Director of CSIS in June 2017. The Director oversees the overall management of the Service, and has formal responsibilities under the *CSIS Act*, including seeking the Minister’s approval and applying for judicial authorizations for investigative activities and threat-related measures. The Director reports to the Minister of Public Safety and is supported by three Deputy Directors representing Operations, Policy and Administration. Mr. Vigneault previously served as the Assistant Secretary to Cabinet, Security and Intelligence at the Privy Council Office (**PCO**) from 2013-2017.

Marie-Hélène Chayer is the Executive Director of ITAC. She works under the authority of the Director of CSIS and the National Security Intelligence Advisor (**NSIA**). As the Executive Director, Ms. Chayer is responsible for the day-to-day operations and management of ITAC, for reporting on terrorism-related events occurring in Canada and around the world, and for assessing the National Terrorism Threat Level (**NTTL**) within Canada.

Michelle Tessier is the Deputy Director, Operations (**DDO**) of CSIS. The DDO of CSIS is essentially the most senior intelligence officer in the agency, and is responsible for the management of operational activity of the Service. Ms. Tessier has served in this position since December 2018. Her primary responsibilities are to manage the collection, analysis and dissemination of information by Service and to replace the Director as necessary. Ms. Tessier has held both operational and executive roles within CSIS since joining the Service in 1988.

Tricia Geddes formerly served as the Deputy Director, Policy and Strategic Partnerships (**DPP**) at CSIS from April 2020 to June 2022. As DDP, she was responsible for strategic policy development, foreign relations, litigation and disclosure, communications and external review and compliance. She currently serves as Associate Deputy Minister of the Department of Public Safety.

Organizational Structure

CSIS and ITAC

Ms. Chayer explained that ITAC has access to the intelligence produced by its partner agencies, namely, the Department of National Defence (**DND**), the Communications Security Establishment (**CSE**), the Royal Canadian Mounted Police (**RCMP**) and CSIS. A number of ITAC employees are seconded from other federal agencies. ITAC engages in extensive consultation with these partner agencies to produce written products called intelligence assessment briefs or threat assessment briefs. ITAC also considers open source information from academia, think tanks and other organizations such as the SITE Intelligence Group, for instance.

Ms. Chayer (or the Director General of Assessment) personally reviews and signs off on every threat assessment produced by ITAC. In addition, she reviews and recommends changes to the NTTL for final approval to Mr. Vigneault.

Classified ITAC reports are distributed broadly amongst federal agencies, including but not limited to RCMP, Immigration, Refugees and Citizenship Canada (IRCC), Canada Border Services Agency (CBSA), Transport Canada, Privy Council Office (PCO). Unclassified versions of ITAC reports are also shared with partners outside the federal government, such as with some police of jurisdiction. Unclassified reports are placed on a web portal for these agencies to access.

Mr. Vigneault noted that ITAC does not need CSIS authorization for its activities. ITAC is an autonomous organization and has the authority to oversee its own operations. It was created after the September 11, 2001 terrorist attacks to mitigate the risk of compartmentalization in the national security community. While ITAC has access to CSIS's intelligence and is co-located at CSIS, it maintains its own governance structure. Ms. Chayer and an ADM level CSIS colleague both attend the standing meetings of the Assistant Deputy Ministers, National Security Operations (**ADM NS Ops**) but in separate capacities.

Relationship with NSIA and PCO

Ms. Chayer explained that ITAC has a reporting relationship to the NSIA. This relationship is not set out by statute, but rather in policy documents. Ms. Chayer has regular bilateral meetings with the NSIA, Ms. Jody Thomas, and the Assistant Secretary to Cabinet, Security and Intelligence, Mike MacDonald, to discuss the ITAC's assessments and priorities. The NSIA is also the co-chair of the Deputy Ministers, National Security Operations (DM NS Ops) meetings, which may provide strategic guidance regarding ITAC's priorities.

Mr. Vigneault explained that, as the Director of a federal agency, he has a functional reporting relationship with the Clerk of the Privy Council. As the head of the federal civil service the Clerk is responsible for recommending to the Prime Minister the Order in Council appointment of the Director and any performance reviews. This relationship exists in addition to the direct reporting relationship between the Director of CSIS and the Minister of Public Safety set out in the *CSIS Act*. Mr. Vigneault also works closely with the Deputy Minister of Public Safety and the NSIA. He and the NSIA have a close working relationship, including through bilateral meetings.

Ideologically Motivated Violent Extremism (IMVE)

Definition of IMVE

Mr. Vigneault noted that the Service led international efforts to define the concept of Ideologically Motivated Violent Extremism (**IMVE**) in 2018-2019. There are four categories of IMVE: xenophobic violence; anti-authority violence; gender-driven violence; and other grievance-driven violence. Mr. Vigneault explained that the Service shifted away from the use of old nomenclature like left-wing and right-wing extremism to better reflect all the categories that use violence to push their ideologies. Ms. Geddes explained that the timing of the shift to IMVE also coincided with moving away from Islamic extremism and an effort to capture all types of violent extremism. The Service also adopted Religiously Motivated Violent Extremism as a concept at the same time. Mr. Vigneault added that the definition of IMVE does not mirror the Criminal Code definition of terrorism, and that is an important distinction. He gave the example of Alexandre

Bisonnette [the perpetrator of the 2017 Quebec City mosque murders], who met the Service's definition of an ideologically motivated extremist, but who was not charged with terrorism offences under the *Criminal Code*. Mr. Vigneault noted that other countries such as Australia and New Zealand have adopted the IMVE terminology developed by the Service. Ms. Chayer noted that ITAC continues to use the IMVE framework and lexicon with international partners for consultation.

Almost half of the Service's counter-terrorism resources are dedicated to IMVE and the need for additional resources continues to grow. The Service has publicly disclosed this statistic in an effort to demonstrate to Canadians that the greatest terrorism threat no longer originates from organized, religiously motivated violent extremism but from IMVE, such as white supremacists and similar extremists who disproportionately target women and racialized minorities.

Operations

Ms. Tessier noted that the IMVE mandate is carried out through operational management and collection as well as through strategic analysis in the form of written products for circulation amongst security partners.

When asked, Mr. Vigneault noted that there are no Ministerial Directions [directions from the Minister of Public Safety to CSIS] in place specifically with respect to IMVE, nor has CSIS made any recommendation to the Minister that such a direction should be made.

Online Rhetoric and IMVE

Mr. Vigneault explained that the ecosystem of IMVE is complex and it is important for Canadians to understand IMVE, including what it is and what impact it has. One aspect of IMVE is the link to conspiracy theory. There are all kinds of conspiracy theories, absurd facts and people use them to leverage their views or create their own narrative. One of the main challenges associated with the IMVE mandate is distinguishing between credible threats to violence that are ideologically motivated, and online rhetoric that is violent or that may constitute hate speech. Mr. Vigneault used the image of a funnel to depict the social context of IMVE, and the associated mandates of law enforcement and CSIS.[1] The largest part of the funnel includes acts and language that may be 'awful but lawful'. In the middle, there is online and real-world content that may meet the legal definition of hate speech and be criminal in nature. The online and real-world activities that meet the s. 2(C) CSIS Act threshold sits at the narrowest part of the funnel. He noted that CSIS and its partners' understanding of IMVE is still evolving. There is a need for early intervention by actors other than national security agencies, such as municipal, provincial and law enforcement agencies.

Ms. Tessier clarified that CSIS is not investigating the Anti-Public Health Measures Movement (**APHM**); it investigates IMVE. CSIS uses three criteria to identify IMVE; 1) Ideologically motivated; 2) intent for societal change, 3) intent to use or promote serious

[1] TS.CAN.001.00000001.

violence to attain change. APHM would only qualify as a form of IMVE if it is part of a larger sociological view of societal change and seeks to use or promote serious violence to attain that change. If it met these criteria, it would fall under the “anti-authority driven violence” subcategory of IMVE.

Ms. Chayer added that it is also very difficult to assess the intent and impact of online violent rhetoric for both the speaker and the receiver of such rhetoric. The anti-government violence umbrella of IMVE can be disparate and individuals might be inclined to act upon a call to violence, but based on their own distinct grievances.

Ms. Tessier noted that this is not an obstacle faced by CSIS alone. Many of the Service’s foreign partners are also struggling to define terms in the IMVE milieu, and to understand the pathway from consuming and posting violent online rhetoric, to radicalization, to violent action. Mr. Vigneault explained that the qualitative and quantitative difference of IMVE today as compared with previous iterations is the use of the internet and in particular, social media platforms. These platforms have allowed people to access content and connect globally to facilitate the circulation of ideas, including conspiracy theories, misinformation and IMVE theories such as the Great Replacement Theory. Mr. Vigneault explained that misinformation consists of the repackaging of truth and facts in a misleading way to further a particular narrative, where as disinformation consists of a deliberate attempt to create alternative or false realities. Where disinformation or misinformation attempt to engage others to participate in serious violence for a political, religious or ideological objective or relate to foreign interference, then it falls within CSIS’s mandate.

Intelligence Collection Pertaining to Protests

Intelligence

Mr. Vigneault stated that at no point did the Service assess that the protests in Ottawa or elsewhere [those referred to as the “Freedom Convoy” and related protests and blockades in January-February 2022] constituted a threat to the security of Canada as defined by section 2 of the *CSIS Act,* and that CSIS cannot investigate activity constituting lawful protest.

Ms. Tessier and Mr. Vigneault explained that the Service had subjects of investigation who showed interest or participated in the convoy.

Mr. Vigneault emphasized that the threshold imposed by the *CSIS Act* and under which the Service operates is very specific. For example, the determination that something may not constitute a threat to national security under section 2 of the Act does not preclude a determination that a national security threat under a broader definition, or from the perspective of the public, does exist.

Threat Assessments

Ms. Chayer recalled that the ITAC produced its first terrorism threat assessment pertaining to the convoy on January 26, 2022.[2] In preparing its assessments, ITAC considers if the three factors of intent, capability and opportunity for violence are present. ITAC has a detailed methodology by which it assesses the NTTL, which includes consideration of mitigation factors but it remains the specific assessment of a threat of a terrorist act. During the convoy the NTTL remained at medium. Ms. Chayer explained that this assessment took into account the possibility of violence by rogue actors already involved in the protests and the possibility of random individuals becoming triggered to act violently by the protests. She noted that the lone actor threat is constant, given its unpredictability, but the protests created a "soapbox" effect. This was taken into account in the NTTL determination.

Ms. Tessier noted that the greatest threat of violence, particularly in the context of IMVE, often comes from consumers and not necessarily producers of propaganda. It is difficult to predict the likelihood of lone actor attacks because their communications are not necessarily accessible and because violent rhetoric is becoming increasingly mainstream. Mr. Vigneault added that some attacks or incidents such as the January 6th Capitol Hill attack, have organized elements or command structures however, in the majority of IMVE-related attacks occurring in Canada in the last five years, the perpetrators were not known to one another, but all had engaged with violent online content in some manner.

Ms. Tessier noted that there is a distinction between online rhetoric and ingrained belief but it is not an exact science. We need more than just intelligence agencies dealing with the increasing violent rhetoric in society.

Intelligence Sharing with Law Enforcement

Mr. Vigneault and Ms. Chayer explained that the Service and ITAC participated in two information-sharing tables with law enforcement, namely, the Combined Intelligence Group (CIG) and INTERSECT. [The CIG was established on January 28th. CSIS and ITAC participated daily in the CIG until it was concluded on February 27th. INTERSECT is an emergency response program within the National Capital Region. It is co-chaired by the Ottawa Police Service (OPS), the RCMP and the City of Gatineau.]

At these meetings, CSIS would share and receive information with police agencies such as the OPS and the Ontario Provincial Police (**OPP**). CSIS received more information from police agencies than it shared. Mr. Vigneault recalled that CSIS shared its assessment that there was no threat to the security of Canada under the *CSIS Act* at

[2] TS.NSC.CAN.001.0000156_PR.

these meetings. CSIS did not divulge the intelligence that formed the basis of these assessments.

Mr. Vigneault noted CSIS shared intelligence with the RCMP in accordance with the OneVision framework. This framework allows CSIS and RCMP to de-conflict intelligence and share information without obstructing their investigations. Where possible, the agencies will prioritize the protection of an ongoing criminal investigation above intelligence sharing. For example, CSIS was not directly involved in the RCMP's criminal investigation that resulted in the arrest of four individuals in Coutts, Alberta. Most of the information that CSIS received from the OPS, the OPP and the RCMP was related to public order and potential criminal activity and did not fall within CSIS' mandate.

At the time of the interview, neither Mr. Vigneault nor Ms. Chayer could recall whether they received situational reports from the OPP in early January, or whether they received information from OPP "Project Hendon" operation, however they opined that it is likely that this information was shared with CSIS regional offices given the information sharing arrangements in place.

Ms. Chayer explained that ITAC has ongoing relationships with police of jurisdiction. ITAC shares unclassified reports with police agencies and may receive intelligence from police agencies that have their own intelligence units. When asked, Ms. Chayer could not recall whether the threat assessments prepared by ITAC relied on intelligence from law enforcement or other non-federal agencies.

Foreign Interference

Mr. Vigneault explained that use of the term "foreign influence" under section 2 of the *CSIS Act* refers to foreign state interference, as the term is used within the national security community. CSIS assessed there was no indication of foreign state interference occurring in the course of the protests. CSIS did not assess that any foreign states supported the protests through funding; that foreign states deployed covert or overt disinformation techniques; or that any foreign state actors attempted to enter into Canada to support the protests.

GiveSendGo Data Leak

Mr. Vigneault explained that CSIS did not obtain or consider the list of donors that became public as a result of the GiveSendGo leak in making this determination. The Service's position was that the GiveSendGo donor list did not constitute publicly available information, given that it was the result of a data breach. Therefore, under section 11 of the *CSIS Act*, this information constituted a dataset requiring an application for judicial authorization for its use and retention. The Service decided not to pursue such an application for several reasons, including the data's intelligence value, its analysis by other agencies, and the time required to file an application for a section 11 judicial authorization, which would render the data far less useful. Ms. Tessier further explained that the Service would have sought proper authorization had it assessed there was high value from a national security perspective in doing so.

Mr. Vigneault noted that the experience highlighted the fact that section 11 process could become unworkable in future situations in which information that is publicly known, and that might be necessary from a threat perspective, is not accessible to the Service. The Service intends to seek legislative review of the dataset regime in the *CSIS Act* in the future.

Involvement in Decision to Invoke the EA

Mr. Vigneault noted that CSIS participated in the ADM NS Ops and Deputy Ministers' Operations Committee (DMOC) meetings co-chaired by the PCO and Public Safety at the end of January. These were both standing weekly meetings that were used to coordinate a federal response to the convoy. Ms. Chayer recalled sharing an ITAC threat assessment at the first ADM NS OPS meeting which took place on January 26, 2022. [Mr. Vigneault also attended the Cabinet Committee on Safety, Security and Emergencies held on February 3rd and 6th, 2022.

Recommendation to Cabinet

Mr. Vigneault learned that the EA referenced the threat definition set out in section 2 of the *CSIS Act* once the federal government began to seriously consider invoking the EA [between February 10th and 13th]. He requested that the Service prepare a threat assessment on the risks associated with the invocation of the EA. He felt an obligation to clearly convey the Service's position that there did not exist a threat to the security of Canada as defined by the Service's legal mandate.

The threat assessment prepared by the Service was that the invocation of emergency legislation risked further inflaming IMVE rhetoric and individuals holding accelerationist or anti-government views.[3]

Mr. Vigneault discussed the draft version of this assessment at an earlier meeting of the Incident Response Group (IRG) on February 13, 2022. The document was also available for distribution for the Cabinet meeting. Mr. Vigneault does not know if it was distributed by PCO. The Service did not undertake any similar assessments on the risks associated with the deployment of the Canadian Armed Forces (CAF) or the involvement of DND in the government's response to the protests.

Threshold under EA

Mr. Vigneault explained that, although section 16 of the EA references the definition of a threat to the national security of Canada set out in section of the *CSIS Act,* the two statutes are concerned with distinct issues. The definition of national security is multi-

[3] TS.NSC.CAN.001.00000172_PR.

layered and reaches across government agencies. Mr. Vigneault gave the example of the ADM NS Ops, which includes the participation of various federal agencies including Transport Canada, DND, CAF, IRCC, CSIS, and Public Safety, all working within their practical and operational definitions of national security. Another example is the COVID-19 pandemic, which can be defined as a national security threat, but not from the perspective of the *CSIS Act*. He further explained that the EA cannot be read in a manner that gives CSIS the exclusive authority to determine whether there exists a public order emergency, as this is the responsibility of the federal government.

Mr. Vigneault further explained that the section 2 definition of a threat to the security of Canada is in need of modernization. This provision was enacted nearly forty years ago and there is a need for mature, public discourse around the reform of national security legislation.

Emergency Measures

When asked, Mr. Vigneault explained that CSIS did not request any specific measures under the EA. It did not benefit from any new authorities under the EA. CSIS did not receive any reports from FINTRAC pursuant to the EA Regulations or the Emergency Economic Measures Order.

Section 58 Explanation

When asked, Ms. Geddes explained that the Service had limited involvement in the drafting of the Section 58 Explanation. The Service provided general input onto a very late draft of the Explanation, which did not identify the sources of information. Mr. Vigneault noted that CSIS did not provide the information on page 12 of the reasons pertaining to the increase in online rhetoric by US based individuals, or the references to the participation of US-based individuals in the convoy, or the increase in threats to elected officials since the convoy began.

Impact of Invocation on IMVE

Mr. Vigneault explained that the Service has not changed its approach to monitoring IMVE since the invocation of the EA in February. It continues to maintain a posture of “heightened awareness” and has noted an increasing amount and intensity of IMVE rhetoric, however not necessarily as a result of the convoy.

Lessons Learned

The panelists identified several general areas for policy reform and improvement related to CSIS’ authorities and general ability to investigate threats to the security of Canada, regardless of the protests. Ms. Geddes noted that one gap is in Service’s warrant regime, which only provides a ‘one size fits all’ warrant threshold even for less intrusive surveillance measures. There are also the challenges and limitations posed by the section 11 dataset regime. Another issue faced by the Service is the sharing of classified information with non-government entities without the use of special bridge authorities. Another longstanding challenge identified by Ms. Geddes is intelligence and evidence, and the difficulty in sharing information with law enforcement that can be used in criminal proceedings while also protecting sensitive sources. One issue that was relevant to the protests identified by Mr. Vigneault is the critical gap in the regulation of online violent rhetoric. He noted that this was not an appropriate task for the Service or for any national security agency, generally speaking, to be involved in (given the constitutional implications). However, there is a critical need for a civilian government institution to monitor and regulate social media and to address the increase in violent online rhetoric before it reaches CSIS's threshold.

Mr. Vigneault also observed that some processes worked very well during the protests. He noted that there was good information flow and coordination amongst federal agencies due the use of the IRG. Both Ms. Tessier and Mr. Vigneault were free to speak, advise and convey their positions and assessment directly to the decision-maker.