Interview Summary: David Vigneault (Canadian Security Intelligence Service), Alia Tayyeb (Communications Security Establishment), Daniel Rogers (Privy Council Office)

Background

Senior officials from the Canadian Security Intelligence Service, Communications Security Establishment, and Privy Council Office were interviewed in a panel format by Commission counsel on January 16, 2024.

The interview was held in a secure environment and included references to classified information. This summary has been drafted in a way that removes or summarizes classified information so that the summary can be disclosed publicly.

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 activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, and report to and advise the Government of Canada on such threats. The *Canadian Security Intelligence Service 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 measures to reduce threats to the security of Canada.

David Vigneault was appointed Director of CSIS in June 2017 and was reappointed in this position in June 2022. The Director oversees the overall management of the Service, and has formal responsibilities under the *CSIS Act*, including seeking the Minister's approval in applying for judicial authorizations for investigative activities and threat reduction 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 from 2013–2017.

The **Communications Security Establishment** is Canada's national cryptologic agency, providing the Government of Canada with foreign signals intelligence and also houses the Canadian Centre for Cyber Security. Its core mandate is defined by the provisions of the *Communications Security Establishment Act* ("*CSE Act*"). CSE collects foreign intelligence from the global information infrastructure primarily through communications and other electronic signals, referred to as signals intelligence ("SIGINT"). CSE uses SIGINT to produce foreign intelligence reports.

Alia Tayyeb was appointed Deputy Chief, SIGINT at CSE in 2022 and in this capacity is also responsible for the foreign cyber operations aspect of the CSE mandate. She held other positions within CSE, PCO and CSIS prior to this appointment.

The **Privy Council Office** ("PCO") is the central government office that supports the development and implementation of the Government's policy and legislative agenda, and coordinates the responses of all Canadian government departments and agencies. In the national security context, the National Security and Intelligence Advisor to the Prime Minister ("NSIA") Branch, which includes the Foreign and Defense Policy

Secretariat, the Security and Intelligence Secretariat, and the Intelligence Assessment Secretariat, is an integral part of PCO, amongst others.

Dan Rogers was appointed Deputy NSIA in May 2023. In his role as Deputy NSIA he is involved in the coordination within government with respect to national security. He and the NSIA act as advisors to the PM and Cabinet on national security matters and as liaisons with other foreign governments and the intelligence community. Mr. Rogers previously served as Associate Chief of CSE, as Deputy Chief SIGNET at CSE, as Director of Operations for the Security and Intelligence Secretariat at the PCO, and as Director of SIGINT Programs Requirements at CSE.

Legal Authority to Disclose Classified Information

CSIS & CSE

Mr. Vigneault explained that CSIS is statutorily limited in its ability to disclose classified information. For example, sections 18 and 19 of the *CSIS Act* prohibit the disclosure of classified information except in certain defined circumstances. Section 19 limits the disclosure of classified information outside of the Government of Canada, except where such disclosure is required as a part of CSIS's threat reduction measures or as required by law. Sections 18 and 18.1 prohibit, respectively, disclosure where it may lead to the identification of a CSIS employee or a human source. Within the Government of Canada, disclosure of classified information can generally occur when the recipient has the appropriate security clearance and needs to know the information contained in the classified materials.

Ms. Tayyeb noted that there is no specific provision of the *CSE Act* that provides legal authority to disclose classified information. She further explained that the structure of the *CSE Act* allows for activities to keep operations covert. Furthermore, section 55 of the *CSE Act* bars the disclosure of information that could reveal the identities of individuals or entities that assist CSE in its mandate on a confidential basis. CSE relies on the voluntary assistance of its partners to execute its mandate, which is covert by nature.

Both Mr. Vigneault and Ms. Tayyeb noted that the *Security of Information Act* ("*SOIA*") permanently binds most CSIS and CSE employees to secrecy. Both underscored that the need to protect classified information is implicit in the structure of *SOIA*.

Mr. Rogers explained that the Treasury Board's Policy on Government Security determines how information should be classified and handled. This in turn governs the manner in which an agency is to handle classified information.

Sharing Intelligence with Domestic and Foreign Partners

CSIS

Mr. Vigneault explained CSIS shares intelligence with domestic and foreign partners. On the domestic side, CSIS shares intelligence with federal government partners. This sharing is governed by internal policies. Mr. Vigneault noted that s. 19 of the *CSIS Act* restricts the disclosure of the information it collects, as explained above. CSIS also shares intelligence with foreign partners pursuant to s. 17 of the *CSIS Act.* CSIS maintains over 300 relationships with foreign entities under this authority.

CSE

Ms. Tayyeb noted that information and intelligence sharing with domestic partners is central to CSE's capacity to fulfill its mandate. The *CSE Act* allows the organization to distribute its products for consumption by other federal government agencies. The *CSE Act* also provides CSE with the authority to enter into arrangements with foreign partners. In practice, CSE shares information primarily with its Five Eyes partners. [The Five Eyes is a partnership, dating back to the Second World War, that was created for the facilitation of intelligence sharing between Canada, the United States, the United Kingdom, New Zealand, and Australia].

For its part, the Canadian Centre for Cyber Security ("Cyber Centre") [a branch of CSE] has the ability to enter into arrangements with different foreign and domestic partners. That said, given the nature of Cyber Centre's mandate, which includes the issuance of public advisories about cyber-security issues that might affect the public, the Cyber Centre issues many unclassified products for the Canadian public and private industry.

Intelligence Products

CSE

Ms. Tayyeb explained that CSE's main output is a type of report that puts intelligence into a narrative form for consumption by government officials or other partners. These reports are summaries that do not necessarily contain detailed analysis or assessment. CSE also produces analytical reports. CSE reports may be directly distributed across government agencies, with CSIS being the primary consumer of CSE's reports, and they may be distributed within the Five Eyes as required. CSE reports can be sanitized

to limit the disclosure of sensitive information, depending on the recipient. [Sanitization is a process by which sensitive information is removed from a document to allow for wider distribution]. Finally, CSE creates an annual report which provides the public with an overview of its activities and operations.

PCO

Mr. Rogers explained that the PCO produces assessed all-source intelligence products through the Intelligence Assessment Secretariat (IAS). That is to say, PCO will assess both classified and open-source information in creating its intelligence products. The volume of reports created by PCO is smaller than that of products created by CSIS or CSE, because PCO does not collect its own intelligence and its reports are generally created for a specific purpose. For example, PCO may create a document to advise the Prime Minister before a foreign engagement. Otherwise, the IAS creates daily products for wide circulation within PCO and weekly briefs for the Prime Minister and other Ministers concerned with national security.

Mr. Rogers also noted, by way of example, that the Security Intelligence Threats to Elections Tasks Force ("SITE TF"), produces intelligence products. However, the SITE TF is a multi-agency body because its reports reflect the collaboration of representatives from Global Affairs Canada ("**GAC**"), PCO, CSIS and CSE.

CSIS

As part of CSIS' mandate is to collect intelligence and provide information to Government, the intelligence products created by CSIS include raw intelligence. In this context "raw intelligence" means information collected by CSIS that has not been assessed in its full context, i.e., in conjunction with other relevant information or

intelligence. CSIS may distribute this raw intelligence to partner agencies if it is relevant to that agency's mandate or intelligence requirements.

Mr. Vigneault explained that since CSIS' mandate is to report to and advise the government of threats to the security of Canada, the majority of what CSIS produces are classified intelligence products that range from the distribution of the above-noted reports with contextual information to comprehensive intelligence assessment products. These products are drafted for specific individuals who have the appropriate security clearance and a need to know the information contained in the product. Often, these products specify a restricted list of individuals to whom the document may be distributed. CSIS products will generally provide some explanation of the source of the information, including whether the information is corroborated or uncorroborated.

These products, given their content, cannot be publicly disclosed without the redaction of all classified information. In some cases, unclassified information in a product may be redacted, if that unclassified information could reveal something about the classified information in the product. Generally, information is redacted because it might reveal something about a CSIS source, an ongoing investigation, or other sensitive information that CSIS cannot make known without compromising its operations and Canadian national security. The specificity of information in the CSIS products generally results in the requirement that more information requires redaction/protection before the product can be disclosed.

CSIS also creates documents called "placemats". Placemats are generally one-page documents that synthesize information into graphically arranged short narratives to help the recipient understand the intelligence described. These documents are usually

drafted for individuals with specific security clearances, and are classified according to the sensitivity of the information or intelligence contained in them.

CSIS also creates intelligence assessment products. Intelligence assessments collect information from other intelligence products and use it to describe an intelligence issue or formulate an answer to an intelligence question. This generally occurs where a specific individual or agency has manifested an interest in understanding a situation and has requested that CSIS respond. Again, if these documents were to be disclosed, it would be necessary that they be redacted to prevent the disclosure of all sensitive information.

Finally, in briefing Ministers, CSIS may generate briefing notes drawing upon a combination of reports and products, as required.

Designating Classification Level

CSE

Ms. Tayyeb explained that CSE has various standards in place that dictate what classification level should be applied to its various intelligence products. These well-established standards were developed in conjunction with CSE's Five Eyes partners. Generally, the author or originator of the intelligence product sets the classification level according to the applicable standards.

Ms. Tayyeb noted that where CSE receives information from foreign partners, the foreign partner designates the classification of the intelligence product shared. It is imperative to respect the classification levels set by foreign partners to preserve the relationships with these foreign partners and foster information sharing.

As it relates to SIGINT, most of CSE's products are designated Top Secret/Special Intelligence. Ms. Tayyeb explained that a document containing particularly sensitive information may be designated in a category that results in even more restrictive access than a Top Secret classification.

Generally speaking, a classification level limits distribution of sensitive information. A classification level aims to reduce risk and ensure the accountability of the agency that receives the product to which the classification is applied. CSE can apply a process to sanitize or lower the classification of a document but this will necessarily remove detail and information from its contents.

CSIS

Mr. Vigneault explained that CSIS also sets classification levels by using well-established agency standards established by policies. Typically, the level of classification applied to an intelligence product is correlated to the level of harm that would arise if the intelligence product was disclosed. This harm could be to an individual, such as a human source, or to other aspects of an ongoing investigation. In every situation, the level of classification is determined by professionals within CSIS such as subject matter experts who understand the context of information and the level of protection required.

Further, Mr. Vigneault underscored the need to apply rigorous protection to information that reveals human sources. It is imperative that CSIS protect this information, to protect the safety of the sources, to ensure continued access to the sources, and to preserve CSIS's ability to recruit other sources.

PCO

Mr. Rogers explained that, because PCO does not collect intelligence on its own, it does not apply its own classification levels to intelligence products. Instead, it reflects whatever level of classification the originating agency (e.g., CSE, CSIS) applied to the intelligence product. Mr. Rogers also explained that Canada inherits the classification of information provided by foreign partners.

Disclosure of Information or Intelligence

Disclosure Requests and Risks to National Security

Ms. Tayyeb explained that CSE has a team that deals with requests for disclosure of information. The team deals with declassification, litigation requests, access to information requests, policy, and compliance. When answering disclosure requests, the team must consider the need to preserve CSE's access to information. CSE cannot disclose information that would reveal its interest in a target, that it has access to a target's information, or how it accessed that information. Disclosing this information could enable a target to use countermeasures or otherwise compromise CSE's ability to gather information and intelligence. Disclosure is generally possible only when the source of the intelligence cannot be learned from the information disclosed.

Ms. Tayyeb also underscored the need to protect the information of CSE's foreign partners. CSE cannot disclose information that would reveal foreign partners' methods, techniques, or aims. [CSE cannot disclose information from a foreign partner without the partner's consent.] Otherwise, CSE risks jeopardizing its relationship with these partners. Finally, Ms. Tayyeb emphasized the need to protect the safety of Canadians.

Some information, if disclosed, could also reveal the identity of CSE employees or other individuals. Mr. Vigneault agreed with the comments made by Ms. Tayyeb.

Mr. Vigneault underscored that in the age of big data, it is possible for adversaries to gather small pieces of seemingly unrelated information, put these pieces of information together, and learn things about CSIS sources or techniques that would have otherwise remained hidden from them.

All three witnesses explained that the more specific a piece of information, the easier it is for an adversary to use it to identify a source or technique. Thus, typically the risk to national security is higher when the information is about specific intelligence than intelligence of a more general nature.

Resource-Intensive Requests

All three witnesses explained that disclosure requests are resource and labour-intensive. When a disclosure request is made, experts in legal processes must deal with the request and the legal parameters surrounding it. Subject-matter experts must examine each piece of information to ensure that revealing the information will not cause injury, directly or in conjunction with other information that is or might in the future be known to the public. These subject-matter experts are people who have the relevant background to understand whether disclosing information will be injurious given the context.

Mr. Vigneault stated that it is important that our institutions remain as transparent as possible for public engagement and trust. CSIS has dedicated units that support disclosure requirements that come from police investigations, Federal Court

proceedings, requests by review agencies (NSIRA and NSICOP) and ATIP requests. Those units also consult with subject matter experts to assess the potential national security injury of a disclosure. As a result, disclosure requests require considerable work and resources. For example, it took 200 person hours to redact the 13 sample documents requested by the Commission. A large number of these requests can tie up valuable resources and impact an agency's ability to perform its mandate. It is not in the public interest to compromise an agency's ability to do its work and protect Canadians.

There are no pre-existing arrangements with foreign partners through which a Canadian agency could disclose foreign intelligence without the consent of the originator. Requests for disclosure of foreign sourced intelligence are made on a case-by-case basis. Mr. Vigneault cautioned that if a Canadian intelligence agency makes too many requests to disclose information given to it by foreign partners, these partners may re-evaluate information-sharing arrangements. He also noted that when disclosure requests relate to intelligence obtained from foreign partners, Canadian agencies do not control the timeline for redactions and disclosure.

"Writing to Release"

All three witnesses explained that, in some circumstances, information or intelligence gathered by various agencies can be "written to release". This means that the agency (e.g., CSE, CSIS) will draft a narrative of the underlying intelligence intended for public release. This is often more efficient and effective than redacting documents individually. As an example, SITE TF participants used the "write to release" approach for the reports it issued during a by-election. They knew a public report would have to be released, so they drafted intelligence in such a way as to be publicly disclosable.

Generally speaking, Ms. Tayyeb explained that CSE will sometimes "write to release" instead of redacting a document that has been written at the highest classification level. This is because so few individuals are cleared to receive reports at the highest classification. Writing to release allows the information to be circulated to those who need to know it without compromising highly sensitive collection techniques or other information a recipient does not need to know. CSE will also "write to release" time-sensitive information and information related to public safety threats.

Mr. Vigneault explained that CSIS has "use letters" that are drafted to be conveyed to law enforcement to allow them to begin investigations into potentially criminal matters that have come to CSIS's attention. He noted that there is no government policy for converting classified information into information that can be publicly disclosed. Instead, CSIS determines whether something should be written for release based on its intended recipients and the sensitive nature of the information to be disclosed.

The Declassification Process

Challenging a Redaction

Ms. Tayyeb noted that decisions related to changing or revising a redaction are made by officials on the recommendation of subject-matter experts. The level of the decision-maker depends on the circumstances, but in the context of this Inquiry, that is elevated to the level of Assistant Deputy Ministers or Deputy Ministers (or equivalent rank), depending on the circumstances. Generally, any process related to changing or revising a redaction will involve balancing the public interest in disclosure against the risk of injury that may result from its disclosure. She stated that disclosing sensitive information about sources and methods may impact an intelligence agency's ability to obtain threat

information in the future. She highlighted that there is a strong public interest against disclosure in these types of situations because the loss of future threat information damages CSE's ability to protect Canadians.

Mr. Vigneault explained that it would be extremely unlikely that a redaction covering information that could identify a human source would be lifted, even if the matter was raised to him for decision. It is important that CSIS be able to protect its sources and against a chilling effect that would occur if CSIS were not able to effectively protect its sources. This result would jeopardize the ability of CSIS to fulfill its mandate. Mr. Vigneault suggested that there may be a mistaken belief that maximum transparency is always in the public interest. He noted that there is no dichotomy between restricting disclosure and the public interest because CSIS' mandate is to protect Canada's national security. Thus, it is sometimes in the public interest to restrict disclosure to the extent that doing so is necessary to allow CSIS to fulfill its mandate.

Mr. Rogers explained that public servants entrusted with classified information are duty-bound to protect that information. They strive to act in the public interest. Although transparency serves the public interest, there is also a public interest in the protection of this information as open dissemination could have a significant impact on the Government's ability to protect Canadians in the future.

Impact of Unauthorized Releases

Damaged Public Trust in Institutions

Mr. Vigneault explained that unauthorized releases of information can harm public trust in the intelligence community and in democratic institutions. It can also impact the

Canadian intelligence agencies' relationships with international partners, and result in international partners restricting the information they share with Canadian agencies. Unauthorized releases also impede intelligence collection capabilities and undermine ongoing investigations. Furthermore, unauthorized releases have an effect on the trust of Canadians in the ability of federal institutions to protect their information.

Mr. Vigneault and Ms. Tayyeb explained that unauthorized releases of information prevent the intelligence community from having conversations with the public about how intelligence institutions work and may give the public a partial picture of the whole. This can lead the public to draw false or misleading conclusions about an institution and its operations.

Lack of Critical Context to Understand Information

Mr. Rogers explained that information or intelligence that is the subject of an unauthorized release was generally crafted for a specific audience with a specific background of information and expertise. That audience has the context and experience needed to understand and assess the reliability and completeness of the information or intelligence provided. That audience can also consult with the originating agency to clarify ambiguities or misunderstandings. In most cases, the public does not have this critical context, nor does it have the ability to clarify ambiguities or misunderstandings. When viewed out of context, information that is subject to an unauthorized release can be misunderstood or misconstrued by the public, leading to further harm.

Ms Tayyeb concurred that the lack of context around information or intelligence that has been the subject of unauthorized release may give the wrong impression to a person without the full context.

Mr. Vigneault explained that the public is often unable to critically assess the contents of a classified report and is at risk of attributing too much significance to its contents. He emphasized that intelligence is not evidence and that it takes a trained intelligence professional to interpret a CSIS intelligence product. Further, Mr. Vigneault explained that the fact that there has been an unauthorized disclosure does not provide the agency with the ability to comment on the contents of that disclosure in a public forum. Thus, CSIS' ability to clarify misunderstanding in the context of unauthorized disclosures is limited.

The Foreign Interference Context

Mr. Vigneault distinguished foreign interference from espionage with reference to the human element. Foreign interference often involves foreign actors pressuring or threatening human beings. Foreign interference is a concept that extends beyond elections and democratic institutions. It has the potential to harm individuals and has resulted in individuals being harmed.

Information Collection

Mr. Vigneault explained that intelligence collection in the foreign interference context runs the gamut. CSIS will collect information from contact with members of the public, but it will also collect information from highly sensitive sources. Some information is unclassified, and some information is highly classified.

Sophisticated Parties

Ms. Tayyeb and Mr. Rogers noted that intelligence collection in the foreign interference context is also distinct from other intelligence collection because of the sophisticated

parties involved. Foreign interference involves state actors. These state actors are well-resourced and have extensive capabilities. They may be able to detect investigative techniques more easily through disclosure than would be possible by less sophisticated actors.

Mr. Vigneault underscored that some foreign actors do not have the same democratic limitations as Canadian institutions and have vastly greater resources. This means these actors have different capabilities.

PCO Structures and Functions Relevant to Foreign Interference Context

Internal Structures

Mr. Rogers described the internal structures within PCO that relate to foreign interference. He explained that the NSIA convenes and coordinates the Canadian intelligence community, and advises the Prime Minister and Cabinet on national security issues.

The NSIA supports the Prime Minister and Ministers, including the Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs, in part by convening the security and intelligence community on national security issues. The Democratic Institutions Secretariat works to strengthen Canada's electoral system, including through initiatives such as the Critical Elections Incident Public Protocol and the SITE Task Force.

Relevant Products

Mr. Rogers explained that PCO does not produce one standard type of intelligence product related to foreign interference. As noted above, PCO produces all-source

assessments and may produce written or oral briefings for the Prime Minister or Cabinet or memoranda to Cabinet. If PCO receives a CSIS summary or assessed product, it might provide that product to the Prime Minister or Cabinet. Mr. Rogers emphasized that PCO is generally a consumer, rather than a producer, of intelligence.

Information Sharing by PCO

Mr. Rogers states that PCO is bound by the same system of information handling as other members of the intelligence community. It will not provide classified materials to individuals who do not have the appropriate security clearance and / or indoctrinations. [Indoctrinations are security briefings required to access certain types of information. Individuals who are indoctrinated to a specific type or topic of classified information will undertake to protect that information in accordance with the applicable law and policy.]

If an individual does not have the appropriate clearance and / or indoctrination, but PCO needs to communicate certain classified materials to them, PCO will sometimes initiate a process to get that individual the appropriate clearance and / or indoctrinations. Alternatively, PCO will consult with the agency that originated the classified materials to determine whether the information can be sanitized to a lower level of classification by removing injurious information or communicated in a different manner that respects classification levels.

In a hypothetical situation where the Prime Minister wanted to brief a wider audience on classified materials, PCO could work with the agencies that originated the classified materials to tailor the information in a way that would remain accurate but not be injurious.

Policies on Authorized Disclosure

Mr. Rogers explained that the NSIA, as a coordinator within the intelligence community, can advise the Prime Minister on policy matters relating to the authorized disclosure of classified information, but does not have any decision-making power with respect to the policies on disclosure of classified information. The power to create policy in this domain rests with the agencies themselves and the Treasury Board.