CANADIAN SECURITY INTELLIGENCE SERVICE
INSTITUTIONAL REPORT

PREPARED FOR
THE PUBLIC INQUIRY INTO FOREIGN INTERFERENCE
IN FEDERAL ELECTORAL PROCESSES AND DEMOCRATIC INSTITUTIONS

In response to the request from Public Inquiry into Foreign Interference In Federal Electoral Processes And Democratic Institutions (Commission) for an Institutional Report in advance of hearings addressing the impact of foreign interference on the 43rd and 44th general elections and on the flow of related information to senior decision makers, the Canadian Security Intelligence Service (CSIS or the Service) is pleased to offer the following responses to your request.

(1) An Overview of the Department or Agency's Mandate.

Established in 1984, the CSIS is a civilian security intelligence service. CSIS' mandate, authorities, thresholds, responsibilities and limitations are enshrined in law by the *Canadian Security Intelligence Service Act (CSIS Act)*.

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

The term "threats to the security of Canada" is defined in section 2 of the *Act* to mean:

- (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage;
- (b) foreign-influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person (a key example being foreign interference (FI));
- (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state; and
- (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada.

Section 2 further specifies that "threats to the security of Canada" "does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d)."

Pursuant to section 12.1 of the *Act,* CSIS may take measures to reduce these threats in certain circumstances, particularly where the required legal conditions under the Act are satisfied.

Section 13 authorizes CSIS to provide security assessments on individuals who require access to classified information or sensitive sites within the Government of Canada.

Section 14 authorizes CSIS to provide security advice relevant to the exercise of a power or performance of a duty or function under the *Citizenship Act* or the *Immigration and Refugee Protection Act*.

Section 15 authorizes CSIS to conduct such investigations as are required for the purposes of providing the aforementioned security assessments (section 13) or security advice (section 14).

Section 16 of the *CSIS Act* mandates the Service to collect foreign intelligence within Canada. Foreign intelligence is that which relates to the intentions, capabilities and activities of a foreign state, a group of foreign states or any foreign person. The Act stipulates that CSIS may only collect such intelligence at the personal request of the Minister of Foreign Affairs or the Minister of National Defence and with the personal consent of the Minister of Public Safety.

Section 17 of the *CSIS Act* authorizes CSIS to cooperate with any department of the Government of Canada or the government of a province, or any police force in a province. CSIS' cooperation with these entities must be approved by the Minister of Public Safety. Also pursuant to Section 17 of the *CSIS Act,* CSIS may, with the approval of the Minister of Public safety, after consulting with the Minister of Foreign Affairs, enter into an arrangement or otherwise cooperate with the government of a foreign state or an institution thereof.

Section 19 authorizes CSIS to disclose classified threat information to stakeholders outside the Government of Canada, including with provinces, territories and municipalities, under a specific set of circumstances, including law enforcement actions. Should the Service need to disclose information for the purposes of its duties and functions under the *Act,* section 19 can allow for such disclosures.

Section 21 of the *CSIS Act* authorizes CSIS to apply for a warrant to conduct activities where there are reasonable grounds to believe that a warrant is required to enable CSIS to investigate a threat to the security of Canada or perform its duties and functions pursuant to Section 16 of the *CSIS Act*. The *CSIS Act* requires that the Minister of Public Safety approve warrant applications before they are submitted to the Federal Court.

Section 21.1 of the *CSIS Act* authorizes CSIS to apply for a warrant where there are reasonable grounds to believe that a warrant is required to enable CSIS to take

measures to reduce a threat to the security of Canada, after having received the Minister's approval.

Each of these authorities may used in the identification of, or in response to, the threat of foreign interference.

(2) A description of the programs, policies and procedures that were implemented by each department and agency to respond to both the general threat and the actual incidents of foreign interference associated with the 43rd and 44th general elections.

CSIS programs, policies and procedures are derived from the authorities listed in the preceding section; they are not specific to a threat and apply to all activities of the Service, including the investigative activities of a threat.

The threat of foreign interference is one of the greatest strategic national security threats facing Canada. The *CSIS Act* defines the threat of foreign influence broadly, of which foreign interference in democratic processes and institutions is a subset. Foreign states direct foreign interference (FI) activities toward Canada's democratic institutions and processes, in efforts to achieve immediate, medium-, and long-term strategic objectives. In doing so, they may seek to influence electoral nomination processes, shape public discourse or influence policy positions of elected officials by means of clandestine, deceptive or threating activities. In addition, foreign states conduct transnational repression through monitoring, intimidation and harassment of diaspora communities in Canada in order to achieve their strategic objectives.

Because of its importance, CSIS has ensured a broad operational and analytical capacity exists to investigate, analyze and advise on the threat of foreign influence. The foreign interference threat, including that which may impact an election does not only present itself during, or in the run up, to a general election. The Service has been investigating FI threats, as defined in paragraph 2(b) of the *Act*, since the inception of the Service. As such, CSIS has longstanding investigations into specific threat actors and states who target Canada and Canadians through clandestine, deceptive or threatening means. CSIS also maintains over 300 international partnerships through which the Service can receive intelligence concerning the foreign interference threats other countries are facing. CSIS reports to and advises the Government of Canada of these threats on an ongoing basis, and CSIS takes lawful measures under its threat reduction mandate to mitigate threats to the security of Canada when appropriate.

In periods of heightened threat activity, CSIS may establish ad hoc teams and reporting structures up to the Director dedicated to investigating, analysing and mitigating a threat. Such an ad hoc team and reporting structure was established in CSIS Headquarters in advance of the 2019 and 2021 general elections. This team collated and assessed all relevant threat reporting and distributed it internally and when appropriate to the Security Intelligence Threats to Elections Task Force (SITE), of which CSIS is an operational member. A CSIS regional office also reallocated resources to

create an ad hoc team to address the FI threats leading up to the 2019 general election. Please see Appendix A for details.

CSIS has undertaken efforts to increase public awareness of foreign interference in Canada's democratic processes, including in relation to the 43rd and 44th general elections within the limits of section19 of the *CSIS Act* as described above. This has included providing unclassified explanations of the threat in its annual public reports and public speeches by the CSIS Director, as well as producing unclassified products distributed on its website. Please see Appendix B2. CSIS' Academic Outreach and Stakeholder Engagement unit has met with and discussed the threat of foreign interference with numerous organizations across Canada. CSIS has also provided unclassified defensive security briefings to elected officials at the federal, provincial and municipal levels. These briefings provide the recipient with a basic knowledge of the threat and means to mitigate against it. For a list of protective security briefings given to elected officials, related to the threat or incidence of foreign interference in the 43rd and 44th federal elections and Canadian Democratic Institutions, please see Appendix B.

In engaging with individuals outside of the federal government, CSIS is limited in its ability to share classified threat related intelligence. Therefore, to better address this and other threats, CSIS and the Government of Canada are consulting with Canadians on possible amendments to the *CSIS Act* to allow for more robust information sharing and advice with individuals or entities outside the Government of Canada.

With respect to foreign interference activities aimed at impacting elections, CSIS has undertaken treat reduction measures in order to mitigate the threat directed by foreign states. Additional information can be found in the CSIS response to question 10, below.

As with all investigations, should the Service assess it has collected foreign interference-related intelligence of a potential criminal nature, the Service has the ability to share intelligence with the Royal Canadian Mounted Police (RCMP). The Service and the RCMP use the *One Vision* framework to govern information sharing as both CSIS and RCMP exercise their separate national security mandates. When deciding on the form of information sharing, CSIS takes into consideration (1) the public interest in sharing information; (2) the impact that sharing may have on CSIS's investigations, methodology, and sources; (3) and the impact of any judicial disclosure obligations on CSIS. CSIS and the RCMP, with the assistance of Department of Justice counsel and Public Prosecution Service of Canada (PPSC) counsel as appropriate, may discuss their respective understandings of the foregoing matters and mitigation strategies that attempt to address the public interest in sharing, while minimizing potential adverse impacts on CSIS's ability to fulfill its mandate.

(3) A listing of key executive positions whose responsibilities were related to the matters covered by the Commission's Terms of Reference (a)(i)(A) and (a)(i)(B) in relevant departments and agencies, and the names of their incumbents since September 2018, with descriptions of their duties.

Pursuant to section 6 of the *CSIS Act*, the "Director, under the direction of the Minister, has the control and management of the Service and all matters connected therewith." Supporting the Director in his management of the Service are three Deputy Directors representing Operations, Policy, and Administration, and five Assistant Directors, described below. All of these positions would entail responsibilities related to the matters covered by the Commission's Terms of Reference.

The Deputy Director Operations (DDO) heads the directorate that is responsible for all operational activities of the Service. The DDO reports to the Director and is responsible for several program areas, including intelligence collection, assessments, threat reduction measures and security screening. The DDO is supported by two Assistant Directors. The Assistant Director Collection (ADC) manages and oversees all operational collection activities, both foreign and domestic. The Assistant Director Requirements (ADR) supports the DDO with the overall management and oversight of CSIS' national operational and intelligence requirements, intelligence analysis and dissemination activities. The DDO is responsible for the prioritization of investigative activities, the dedication of resources, and the strategic direction to counter threats, including foreign interference.

The Deputy Director of Policy and Strategic Partnerships (DDP) supports the Director by developing and providing strategic policy advice to the Director as well as managing the Service's strategic partnerships with external stakeholders. The DDP spearheads legislative and policy changes to better respond to the evolving threat of foreign interference. Additionally, the DDP represents the Service at national and international collaborative forums dedicated to national security and intelligence, including countering foreign interference.

For a full listing of key executive positions related to foreign interference during the 43rd and 44th GE and names of their incumbents, please refer to Appendix C.

Additionally, the National Security Litigation and Advisory Group (NSLAG), provides critical legal support and advice to the Service including in legal matters relating to foreign interference. NSLAG is staffed by Department of Justice lawyers who do not come under the direction of CSIS managers. The Assistant Director Legal Services (ADL), a Senior General Counsel from the Department of Justice, oversees NSLAG and ultimately reports to the Minister of Justice.

(4) All means/channels within relevant departments and agencies by which information prepared by intelligence agencies related to possible foreign interference is provided to the Deputy Minister, Minister's office, and Minister. And;
(5) All means/channels by which information related to possible foreign interference is provided from relevant departments and agencies to PCO and PMO.

As part of its mandate, CSIS reports on threats to the security of Canada and provides advice to the Government of Canada, by a variety of means. These responses include through the production of intelligence assessments and reports that are shared with multiple other departments for information purposes, for use in their analysis and to inform their decision-making, and briefings to their executive leadership. CSIS produces thousands of intelligence products on an annual basis, a subset of which is specifically focussed on the threat of foreign interference. CSIS has a robust and secure electronic system for disseminating intelligence products to ensure appropriate readership within the Government of Canada. Other government departments identify their intelligence requirements and the Service responds accordingly by disseminating relevant intelligence to that department.

The dissemination of CSIS intelligence products is governed by a dedicated unit under the ADR. This unit maintains a standard list of designated individuals across government clients who are the primary points of contacts for Service dissemination of intelligence products across all threat topics, including foreign interference. Those designated individuals are responsible for internal dissemination within their organization as they are best-placed to understand the mandate, priorities, and key concerns of their respective organizations. The recipient organizations determine how best to use the intelligence as part of their internal strategic and tactical analyses, briefings, and to guide their program and policy development. There are also CSIS intelligence products with restricted distribution, confined to the named identified recipients. These products contain sensitive information or are from a particularly sensitive source.

This intelligence can be used by the other government departments to brief their Deputy Ministers, Ministers' offices, or Ministers. Government departments must observe the security requirements set out by the Treasury Board to safeguard the intelligence.

CSIS specifically produces assessments, reports, briefing notes, issues management notes, oral briefings and Ministerial Memorandums, for Ministers, Deputy Ministers, the Privy Council Office (PCO) and Prime Minister's Office (PMO). Routine intelligence dissemination occurs through the robust system described above. Oral briefings typically occur through the national security and intelligence governance inter-departmental architecture as described under section 8. CSIS applies its national security and intelligence knowledge, experience and expertise to assess the importance and impact of particular intelligence report and when needed escalate certain pieces of intelligence to the senior decision making levels of Government.

Although briefings are primarily generated by the Service in order to report to advise the Government of Canada, the briefing products described above can sometimes be created in response to other specific government departmental requests. CSIS also responds to ad-hoc requests for meetings from any of the offices mentioned above, as well as contributes regular advice through input into relevant Memorandums to Cabinet and Cabinet discussions.

CSIS meets regularly with the Minister of Public Safety and the Office of the Minister of Public Safety in order to inform the Minister of important national security developments and key elements of the Service's operational activity. These meetings are often oral but can be supported by the provision of intelligence products or memoranda. Emerging issues are flagged according to established protocol for inter-governmental communication. CSIS sends important intelligence products, via the Department of Public Safety, for the Minister's attention.

(6) For each occasion on which there was an oral or written briefing relating to the matters covered by the Commission's Terms of Reference (a)(i)(A) and (a)(i)(B) to the SITE Task Force, the CEIPP panel, a Deputy Minister (or equivalent), the National Security Intelligence Advisor, the Clerk of the Privy Council, PMO or the Prime Minister since September 2018, a listing of the dates, briefing entity and person, including where possible the content of the briefing, and specific cases raised where applicable.
And:
(7) A listing of the dates and subjects covered for each occasion where a department provided advice and/or a recommendation to a Minister or a Minister's office in response to specific intelligence on foreign interference in democratic processes and institutions, including interference in parliamentary business, since September 2018.

CSIS has been investigating FI activities for decades. While the threat from FI has long been present in Canada, its breadth, volume, and impact have grown, making it a significant strategic threat to Canada's national security. As a result, CSIS has been providing briefings on the threat of foreign interference across the Government of Canada, including to senior officials, Cabinet ministers and the Prime Minister.

With respect to the time period in question and in relation to the Commission's Terms of Reference, the Service has provided dozens of briefings to either the SITE, the Critical Election Incident Public Protocol (CEIPP) panel, Deputy Ministers (or equivalent), the National Security Intelligence Advisor to the Prime Minister, the Clerk of the Privy Council, the PMO or the Prime Minister. Please see Appendix D for a listing of these briefings.

(8) A description of the national security and intelligence governance inter-departmental architecture, including Deputy Minister, Assistant Deputy Minister and Director General level committees (e.g. the Deputy Ministers Committee on National Security).

As a means to ensure national security matters, including the threat of foreign interference, are well understood, the Service actively participates in numerous inter-departmental committees. Over the period in question, different committees have been established, some have been discontinued, and some only meet on an ad hoc basis. The full description of the national security and intelligence governance architecture is contained in the Institutional Report of the PCO.

Below is a list of relevant inter-departmental committees on which CSIS is represented. They are not established exclusively to address the threat of foreign interference, but may be required at times to discuss or address the threat, a related intelligence priority, or the dissemination of related intelligence.

<u>Director General (DG) Level Committees</u>

- DG Cyber
- DG Intelligence Assessment Coordination Committee
- DG Intelligence
- DG Election Security Coordination Committee
- DG Hostile Activities by State Actors

<u>Assistant Deputy Minister (ADM) Level Committees</u>

- ADM National Security Policy
- ADM National Security Operations
- ADM National Security Operations Tactical
- ADM Intelligence Assessment Committee
- ADM Intelligence
- ADM Cyber
- ADM Foreign Interference
- ADM Research Security
- ADM Protecting Democracy and Mis/disinformation
- ADM Elections Security Coordinating Committee

<u>Deputy Minister (DM) Level Committees</u>

- DM Intelligence Committee
- DM 5G

- DM China
- DM Clerk
- DM Committee Intelligence Response
- DM Cyber
- DM Elections Security Coordinating Committee
- DM Foreign Interference Committee
- DM National Security
- DM CIP
- DM Operations Committee

(9) A Listing of All Intelligence Products Related to the Threat or Incidence of Foreign Interference in Canadian Democratic Institutions

CSIS uses a variety of domestic and international methods to collect intelligence on individuals and groups whose activities are suspected of constituting a threat to Canada, including the threat of foreign interference. These include, but are not limited to, leveraging open sources, developing contact with members of the public, the recruitment and direction of human sources, means under warrant approved by the Federal Court, arrangements with foreign partners, and arrangements with domestic partners.

This multifaceted intelligence collection is then assessed and analysed to produce a number of different intelligence products used by the Service and the Government of Canada for a variety of specific reasons. The various types of intelligence products serve to inform of significant intelligence or emerging issues, can be to provide an in-depth analysis, provide early insight or additional context on an issue, to provide timely tactical intelligence, or to raise awareness on an issue. Over time, these products evolve but for a full description of the different types of available CSIS intelligence products, please see Appendix E.

Over the period requested by the Commission the Service produced and distributed hundreds of intelligence products related to foreign interference in Canada's democratic processes, at all levels of government. Additionally, the Service has produced many more intelligence products related to the broader foreign interference threat including products on the topic of economics, research and academia. See Appendix F for the list of intelligence products related to the Commission's Terms of Reference.

(10) A Listing of All the Threat Reduction Measures Related to the Threat or Incidence of Foreign Interference in Canadian Democratic Institutions

As noted earlier, CSIS has the mandate to take measures to reduce a threat to the security of Canada in certain circumstances.

The threshold for such a measure is detailed in the *CSIS Act*, which provides: "If there are reasonable grounds to believe that a particular activity constitutes a threat to the

security of Canada, the Service may take measures, within or outside Canada, to reduce the threat."[1] The "*reasonable grounds to believe*" threshold is the same threshold that the Service is required to meet in order to apply for a Federal Court warrant to utilize more intrusive investigative techniques as part of an investigation.

The *CSIS Act* also requires that Threat Reduction Measures (TRMs) must be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures, the reasonable availability of other means to reduce the threat, and the reasonably foreseeable effects on third parties, including on their right to privacy.

CSIS must also consult with other federal departments, as appropriate, with other federal departments or agencies as to whether they are in a position to reduce the threat before taking threat reduction measures as indicated in the *CSIS Act* under subsection 12.1(3). CSIS must also seek a warrant from a judge where a proposed TRM would limit a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* or would otherwise be contrary to Canadian law.

All TRMs undergo a four-pillar risk assessment, completed in consultation with other key government departments, that examines the operational, reputational, foreign policy, and legal risks of proposed actions on a scale of low, medium or high. As assessed risk level rises from low through high, so too does the level of approval required, going from Executive level for low risk to the Director of CSIS and Minister of Public Safety for the highest-risk TRMs. In addition, when assessing the appropriate means of reducing a threat, CSIS considers the range of other possible national security tools available to the broader community, and consults with departments and agencies of the Government of Canada, such as GAC and RCMP, in the approval process as dictated by policy and the risk level of the TRM. Consultation with foreign partners may also be undertaken to reduce any adverse impact on their ongoing operational activities.

As required by the *CSIS Act*, the National Security and Intelligence Review Agency (NSIRA) is notified of all TRMs undertaken by the Service.

In order to reduce the threat from the activities of foreign states conducting foreign interference activities, or to help build resilience to the threat, CSIS has undertaken TRMs related to foreign interference for the period of 2019 01 01 – 2023 09 18. For a full list of TRMs related to the threat or incidence of foreign interference in Canadian Democratic Institutions, please see Appendix G.

[1] *CSIS Act*, s 12.1(1).