

UNCLASSIFIED// NON CLASSIFIÉ

**Public Inquiry into Foreign Interference in Federal Electoral Processes
and Democratic Institutions**

Institutional Report on the Protection of Information in the National or Public Interest

TO: SHANTONA CHAUDHURY
Lead Commission Counsel

Tel: 343-630-3755

Email: Shantona.Chaudhury@pifi-epie.gc.ca

FROM: ATTORNEY GENERAL OF CANADA
Department of Justice Canada
Civil Litigation Section
50 O'Connor Street, Suite 500
Ottawa, Ontario, K1A 0H8
Fax: (613) 954-1920

Gregory Tzemenakis
Senior General Counsel

Barney Brucker
A/Senior General Counsel

Tel: 613-297-2670 / 416-520-4301

Email: JusticeCanada.Inquiry-Enquete@justice.gc.ca

Counsel for the Government of Canada

UNCLASSIFIED// NON CLASSIFIÉ

Contents

1) Canada's National Security Architecture	3
a. Privy Council Office (PCO)	3
i. PCO's responsibilities.....	3
ii. PCO involvement in the S&I community	4
b. Public Safety (PS)	5
i. PS's responsibilities	5
ii. PS's role in the S&I community	5
c. Canadian Security Intelligence Service (CSIS)	5
i. CSIS responsibilities	5
ii. CSIS involvement in the S&I community	6
d. Communications Security Establishment (CSE)	6
i. CSE responsibilities	6
ii. CSE's involvement in the S&I community.....	7
e. Global Affairs Canada (GAC)	7
i. GAC's responsibilities	7
ii. GAC's involvement in the S&I community.....	7
f. Royal Canadian Mounted Police (RCMP)	8
i. RCMP responsibilities	8
ii. RCMP involvement in the S&I community.....	8
2) The Five Eyes Alliance.....	9
3) Protecting information: classifications and dissemination	9
Classified Information - National Interest	9
Protected information.....	10
Classified information.....	10
Control systems.....	10
Indoctrinations	11
Dissemination control	11
Security of Information Act.....	12
Declassification And Sanitization.....	12
4) Protecting information: privileges and immunities	12
Injury to National Security and the need for protection.....	12
Privileges and Immunities.....	13
The Canada Evidence Act ("CEA").....	13
Section 38 of the CEA (NSC).....	14
Statutory Disclosure Restrictions.....	15
Sections 18(1) and 18.1 of the CSIS Act	15
Section 55 of the CSE Act	15

5) Protecting information: redactions and challenges 16

- Internal Litigation Team Process for determining whether information should be redacted, including Positions of those Responsible..... 16
- Internal Department/Agency Process for determining whether information should be redacted, including Positions of those responsible 17
- Internal Process When Commission Questions/Challenges a Redaction, including Positions of those Responsible 17

1) Canada's National Security Architecture

1) A brief overview of Canada's national security architecture, which should describe the relevant agencies/entities and their roles (for instance, the general mandate of each agency/entity; whether it is a collector of intelligence, a consumer of intelligence, or an oversight/review body; and its organizational structure, to the extent that this is relevant to the issues raised at paragraph (a)(i)(D) of the Terms of Reference);

Canada's National Security and Intelligence (S&I) community is made up of multiple departments and agencies, reporting to Ministers and subject to review by several bodies and Parliamentary committees. Each of the departments and agencies has a specific mandate and is governed by its own authorities, policies and procedures.

The key departments and agencies from the S&I community involved in the detection, deterrence and countering of foreign interference directly or indirectly targeting Canada's democratic processes are:

- Privy Council Office (PCO)
- Public Safety Canada (PS)
- Canadian Security Intelligence Service (CSIS)
- Communications Security Establishment (CSE)
- Global Affairs Canada (GAC)
- Royal Canadian Mounted Police (RCMP)

While the roles of producer and consumer of intelligence are not entirely mutually exclusive, in general CSIS and CSE are producers of intelligence while GAC, RCMP, PS and PCO are consumers of intelligence. The S&I community share intelligence as required, within the confines of their mandates, such that each producer of intelligence may also consume the intelligence of other agencies. The Security and Intelligence Threats to Elections Task Force (SITE) is a prime example of this, where each of CSIS, CSE, GAC and the RCMP shared relevant information and intelligence as both producers and consumers.

Parliament has established robust oversight and accountability mechanisms to review the activities of the S&I community, through the National Security and Intelligence Review Agency (NSIRA), the Intelligence Commissioner and the National Security and Intelligence Committee of Parliamentarians (NSICOP). In addition, several Parliamentary Committees, such as the House of Commons Standing Committees on Public Safety and National Security (SECU) and Procedure and House Affairs (PROC), routinely hear matters relating to the S&I community.

The roles, mandates and organizational structure of the key departments and agencies identified above are:

a. Privy Council Office (PCO)

i. PCO's responsibilities

PCO reports directly to the Prime Minister. PCO:

UNCLASSIFIED// NON CLASSIFIÉ

- Supports the development and implementation of the Government of Canada's policy and legislative agendas;
- Supports the Minister of Democratic Institutions;
- Coordinates responses to issues facing the Government and the country;
- Provides security and intelligence-related advice to the Prime Minister; and
- Supports the effective operation of Cabinet.

PCO is headed by the Clerk of the Privy Council, who also serves as Secretary to the Cabinet, Head of the Public Service, and Deputy Minister to the Prime Minister. As a central agency, PCO primarily co-ordinates the work of government departments and agencies, monitoring and developing up-to-date situational awareness on matters related to potential instances of foreign interference.

ii. PCO involvement in the S&I community

a. National Security and Intelligence Advisor to the Prime Minister

The National Security and Intelligence Advisor to the Prime Minister (NSIA) provides policy and operational advice, as well as intelligence, to the Prime Minister and Cabinet on issues related to national security, including foreign interference. The NSIA, Deputy NSIA and supporting secretariats convene the security and intelligence community to ensure the coordination of government responses to all types of foreign interference threats.

With respect to foreign interference, the NSIA is primarily supported by two secretariats: the Security and Intelligence Secretariat (S&I Secretariat) and the Intelligence Assessment Secretariat (IA Secretariat). In addition to information from supporting secretariats, the NSIA relies on information provided by the S&I community, including status updates regarding ongoing security incidents and intelligence on threats to national security.

The S&I Secretariat provides policy advice and support to the NSIA on national security and intelligence matters, including coordinating operational and policy development initiatives for senior-level interdepartmental committees. The S&I Secretariat supports the NSIA in briefing the Prime Minister and Cabinet on key national security issues and has a coordination role whenever national security or intelligence issues are before Cabinet. The S&I Secretariat works closely with Public Safety Canada and other government departments to convene and support regular senior governance meetings on foreign interference threats and responses.

The IA Secretariat is a strategic foreign intelligence analysis and assessment unit. It provides intelligence analysis and assessments to the Prime Minister, Cabinet, Clerk of the Privy Council, and senior Government of Canada officials and plays a key interdepartmental leadership and coordination role for Canadian Intelligence Community assessments. The IA Secretariat also fosters relationships with allied intelligence assessment organizations and builds a stronger allied Intelligence Community through horizontal, community-wide initiatives, enterprise solutions and collaborative, cost-effective intelligence analysis training. The IA Secretariat monitors and assesses foreign interference, examining trends, threats, and emerging issues related to foreign interference as they pertain to the geostrategic environment it covers. The IA Secretariat reports on these issues through its range of intelligence products to its core clients, as well as the broader Canadian S&I community.

b. PCO's coordination role

PCO plays a lead role in coordinating senior public servants, including Deputy Ministers, Assistant Deputy Ministers and Directors General, from various departments and agencies across the S&I community on topic-specific committees.

b. Public Safety (PS)

i. PS's responsibilities

The Department of Public Safety and Emergency Preparedness (PS) is responsible for matters of public safety, national security, and emergency management.

The Department develops and provides advice to the Minister of Public Safety on national security matters in support of the many operational activities undertaken by the Canadian security and intelligence community. This includes functioning as a centralized hub for coordinating work on a number of national security issues, including countering foreign interference.

PS functions as a centralized hub for work in counter-terrorism, critical infrastructure, cyber security and transportation security. PS coordinates and provides support with respect to detection, denial, prevention, response, and recovery on matters relevant to national and cyber security. This includes working with operational and policy partners to provide strategic advice to the Government on evolving and sensitive security issues. PS identifies and works to close gaps in Canada's ability to address and withstand national and cyber-security threats. These threats include, but are not limited to, ransomware, foreign influence, money laundering, terrorist financing, threats to critical infrastructure, weapons of mass destruction, hostile state activity, and terrorism.

ii. PS's role in the S&I community

PS oversees five agencies: the RCMP, CSIS, the Canada Border Services Agency (CBSA), the Correctional Service of Canada (CSC) and the Parole Board of Canada. Of these, the RCMP and CSIS are engaged in efforts to combat foreign interference.

The Minister of Public Safety has the authority to provide direction to the Heads of Agencies, who are responsible for the control and management of their respective agency. Direction is sometimes provided through formal instruments known as Ministerial Directives. Most directions provide high-level direction and require the Deputy Minister or Agency Head to determine the ways and means of accomplishing objectives. In some cases, this is required by law; in other cases, it may still be advisable as an exercise of good governance.

c. Canadian Security Intelligence Service (CSIS)

i. CSIS responsibilities

Established in 1984, the Canadian Security Intelligence Service (CSIS or the Service) is a civilian security intelligence service. CSIS' core mandate is to investigate threats to the security of Canada 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. Among others, s. 2 of the *CSIS Act* defines as a threat to the security of Canada "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," and "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". CSIS' authority to collect information and intelligence on threats to the security of Canada rests primarily in s. 12 of the *CSIS Act*.

UNCLASSIFIED// NON CLASSIFIÉ

Subsection 12(2) clarifies that CSIS may investigate either inside or outside of Canada. Further to its mandate to investigate threats to the security of Canada, CSIS also has the authority under s. 12.1 of the *CSIS Act* to take measures to reduce these threats in certain circumstances.

In addition to investigating threats to the security of Canada, CSIS also conducts foreign intelligence collection within Canada pursuant to s.16 of the *CSIS Act*; that is, intelligence relating to the intentions, capabilities and activities of a foreign state, a group of foreign states or any foreign person. 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.

The head of CSIS is the Director, who serves as Deputy Minister for the organization and reports to the Minister of Public Safety. The Director is supported by several Deputy Directors. The Deputy Director Operations (DDO) is most directly involved in investigating the threat posed to Canada by foreign interference, including in federal elections and democratic processes. The DDO heads the directorate that is responsible for the operational activities of the Service, including intelligence collection, assessments and threat reduction measures. The Deputy Director, Policy and Strategic Partnerships (DDP) is responsible for the overall strategic policy framework of the Service including proposing legislative amendments to the *CSIS Act* so that CSIS can better address foreign interference threats.

ii. CSIS involvement in the S&I community

As Canada's civilian security intelligence service, CSIS collects and assesses intelligence and then provides advice to the Government of Canada, including in the form of intelligence assessments and reports which are shared with other relevant Government of Canada departments for information purposes and for use in their own threat analyses. In 2022, CSIS produced over 2,500 assessments and reports on all threats it was investigating, including foreign interference.

CSIS' intelligence collection activities may serve to advance investigations, assist the Minister of National Defence or the Minister of Foreign Affairs, provide security assessments to departments of the Government of Canada, as well as advice on the admissibility of people to Canada, or to disseminate intelligence, assessments and advice to the government. In carrying out investigations, CSIS may deploy a wide array of operational techniques with varying levels of intrusiveness (e.g., interviews with targets, physical surveillance, and warranted powers to intercept communications or enter premises). When investigations involve Canadian fundamental institutions, CSIS policies and procedures provide additional specific direction, including Ministerial Direction, along with special considerations and enhanced approvals.

d. Communications Security Establishment (CSE)

i. CSE responsibilities

The Communications Security Establishment (CSE) is Canada's national cryptologic agency providing the Government of Canada with foreign signals intelligence (SIGINT), cyber security and information assurance. CSE intercepts and analyzes foreign electronic communications to provide the Government of Canada with unique information about foreign threats to Canadian security and prosperity and important insights to support foreign policy and decision-making. CSE also delivers active and defensive cyber operations for Canada as it relates to international affairs, defence and security, including cybersecurity. CSE's Canadian Centre for Cyber Security helps defend Canadian Federal infrastructure and infrastructure deemed of importance to the Government from malicious cyber activity. CSE provides assistance to federal law enforcement and security agencies, such as CSIS and the RCMP, as well as the Canadian Armed Forces (CAF) and the Department of National Defence (DND) in the performance of lawful duties.

UNCLASSIFIED// NON CLASSIFIÉ

The head of the organization is the Chief, CSE. Chief, CSE serves as Deputy Minister for the organization and reports to the Minister of National Defence (MND). The Chief, under the direction of the MND, has the management and control of CSE and all matters relating to it.

Section 15 of the *Communications Security Establishment Act* sets out CSE's mandate as the national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance. This mandate has five aspects set out in sections 16 to 20: foreign intelligence (s.16); cybersecurity and information assurance (s.17); defensive cyber operations (s.18); active cyber operations (s.19); and technical and operational assistance (s.20).

ii. CSE's involvement in the S&I community

CSE produces over 3,200 signals intelligence reports per year to help support government decision-making in the fields of international affairs, defence and security, including foreign interference, and provides a better understanding of global events and crises and helping to further Canada's interest and security in the world. CSE reports are shared with other relevant Government of Canada organizations (the DND/CAF, CSIS, the RCMP, GAC and PCO, amongst others) for information purposes and for use pursuant to their own mandates. These reports are shared with officials who hold the appropriate clearance and have a need to know.

CSE works with its cryptological partners in the Five Eyes (United States, United Kingdom, Australia and New Zealand). This partnership has endured for over 77 years. Through these and other partnerships, CSE delivers relevant and timely intelligence to satisfy Canada's foreign intelligence requirements.

In addition to also providing cyber security and information assurance services to protect federal infrastructure including blocking close to six billion malicious activities on the Government's network per day, and securing Canada's most valued secrets, CSE provides technical and operational assistance to agencies such as CSIS, the RCMP and CAF. In the course of providing the assistance, CSE operates under the authority of the requesting agency to carry out the activity, including requirements with respect to any applicable warrant.

CSE leverages all aspects of its mandate (foreign intelligence, cybersecurity, foreign cyber operations and technical and operational assistance) to counter hostile state activities, including foreign interference. CSE also works with global and federal partners to mitigate the risks posed by transnational repression activities by gathering SIGINT and by supporting Canada's security and intelligence community. CSE is also an important player when it comes to countering disinformation. Foreign states use disinformation to destabilize Canada's democracy. CSE contributes to government-wide disinformation awareness campaigns, to counter the efforts of foreign interference through online disinformation.

e. Global Affairs Canada (GAC)

i. GAC's responsibilities

Global Affairs Canada, under the leadership of the Minister of Foreign Affairs; the Minister of International Trade, Export Promotion, Small Business and Economic Development; and the Minister of International Development, is responsible for advancing Canada's international relations.

ii. GAC's involvement in the S&I community

Many of Canada's most significant national security threats, including foreign interference, involve a foreign policy nexus. In its work advancing global and regional security interests and managing bilateral

UNCLASSIFIED// NON CLASSIFIÉ

and multilateral relationships, GAC, therefore, contributes to preventing and responding to threats to Canadians and Canadian international interests.

Intelligence on the capabilities, intentions and activities of foreign states collected by domestic and allied intelligence partners informs a wide range of GAC's activities, from policy development to the security of Canada's missions abroad. For example, pursuant to s. 16 of the *CSIS Act*, CSIS may assist the Minister of Foreign Affairs, within Canada, in the collection of foreign intelligence. GAC also produces specialized diplomatic and open-source reporting on foreign interference related issues, as well as strategic intelligence assessments. The CSE Act also foresees that the Minister of National Defence may issue an Active Cyber Operations Authorization only if the Minister of Foreign Affairs has requested the Authorization's issue or has consented to its issue.

f. Royal Canadian Mounted Police (RCMP)

i. RCMP responsibilities

The RCMP is Canada's national police force, with a mandate to prevent crime, maintain peace, enforce laws, contribute to national security, ensure state officials' safety, and provide operational support to law enforcement agencies. The RCMP obtains its authority from several statutes, including the *RCMP Act*, the *Security Offences Act (SOA)* the *Criminal Code* and the common law. Administrative and Operational Manuals, which act as the national manuals for police officers, are among the service manuals that contain the policies, procedures, and protocols that govern the RCMP.

Decision-making and authority falls with the RCMP Commissioner, who is supported by the Senior Executive Committee (SEC), inclusive of the Commissioner, Chief Administrative Officer, Deputy Commissioners, Commanding Officers for British Columbia and Alberta, Chief Financial Officer, Chief Strategic Policy Officer and the Chief of Reform, Accountability and Culture.

ii. RCMP involvement in the S&I community

The RCMP is the law enforcement agency within the Canadian S&I community and works closely with other government agencies and departments to coordinate efforts and address complex issues that require a multi-agency response.

The RCMP is also engaged with key national and international stakeholders seeking to raise awareness of federal priority enforcement areas, including foreign interference, through crime prevention and reporting initiatives. The goal of these efforts is to reduce victimization and increase reporting to police and partners of illicit activities, including foreign interference, that might otherwise go uninvestigated. Those targeted by foreign actor interference may be unaware that they can report these activities to Canadian authorities. The RCMP works with Canadian communities, local police of jurisdiction, in addition to public and private sector entities on these issues.

2) The Five Eyes Alliance

(2) A description of the Five Eyes Alliance;

The Five Eyes (FVEY) alliance is a collaborative intelligence-sharing network comprising five nations: Canada, the United States (US), the United Kingdom (UK), Australia, and New Zealand. It is widely regarded as the world's most significant intelligence-sharing alliance. Established during the aftermath of World War II, FVEY countries collaborate to share a broad range of information and intelligence, and coordinate security efforts, in one of the world's most unified multilateral arrangements. The five member countries have a long history of trust and cooperation, and they share a commitment to common values. The partnership has played a significant role in global security over the past seven decades, strengthening intelligence-sharing and cooperation among its member countries in order to protect their national security and common interests.

The Five Eyes alliance was established for wartime signals intelligence-sharing between the US and the UK. In 1948, the treaty was extended to include Canada, and in 1955, the formal status of the remaining Five Eyes countries was officially acknowledged in a newer version of the UKUSA Agreement.

The FVEY alliance remains one of the most comprehensive and important international relationships for Canada and is built on the mutual respect of each other's laws, the protection of each other's information, and the protection of each other's citizens and nations. Intelligence shared among the FVEY includes signals intelligence (SIGINT), human intelligence (HUMINT), defence and geospatial intelligence, and security intelligence. The extent and range of information shared differs between each of the Canadian agencies and its equivalent partner, and ranges from full interoperability in some cases to transactional sharing in others. Canada is an active contributing member of the alliance and benefits greatly from it. A key commitment of the FVEY is to protect each other's information in accordance with the 'third party rule', which is an understanding that information providers maintain control over subsequent disclosure and use. Canada's non-compliance would risk losing access to the massive amount of critically valuable intelligence the FVEY partners share with Canada.

3) Protecting information: classifications and dissemination

(3) An explanation of the various classifications of protected and classified information used by the Government of Canada;

Classified Information - National Interest

All governments, including Canada's, must maintain a certain degree of security and confidentiality in order to function. The national interest in the proper handling of confidential information can be most acute in cases involving information relating to international relations, national defence or national security. The importance of protecting information the disclosure of which could bring harm to international relations, national defence, or national security has long been recognized by Parliament and by Canadian courts.

Under the Government of Canada's Treasury Board Secretariat's *Policy on Government Security*, sensitive information is controlled by applying appropriate security markings to protect the information therein. The originator of the information is responsible for determining the appropriate marking, which is protected by access controls based on security clearances and indoctrinations. The *Standard on Security Categorization* details the classification markings used

UNCLASSIFIED// NON CLASSIFIÉ

to protect information commensurate with the potential damage to Canadian national interests that could reasonably be expected to occur following an unauthorized disclosure of that information. The categories of protected and classified information are detailed below.

Further, classified information must be dealt with in appropriately accredited security zones. A security zone is an area to which access is limited to authorized personnel and properly escorted visitors. As well, classified information may only be transmitted in accordance with security policies and may only be transported by appropriately cleared individuals using secure containers approved for the level of information to be transported. Finally, there are further restrictions in place in relation to the printing, copying and destruction of copies of classified documents.

Protected information

Applies to information or assets that, if compromised, could reasonably be expected to cause injury to a non-national interest—that is, an individual interest such as a person or an organization. Levels include:

- PROTECTED A: Applies to information or assets that, if compromised, could cause injury to an individual, organization or government. For example, a person's exact salary figure.
- PROTECTED B: Applies to information or assets that, if compromised, could cause serious injury to an individual, organization or government. For example, loss of reputation or competitive advantage, and criminal investigations.
- PROTECTED C: Applies to information or assets that, if compromised, could cause extremely grave injury to an individual, organization or government. For example, catastrophic financial losses or loss of life.

Classified information

Applies to information or assets that, if compromised, could reasonably be expected to cause injury to the national interest, defence and maintenance of the social, political and economic stability of Canada. Levels include:

- CONFIDENTIAL: Applies to information or assets that, if compromised, could cause injury to the national interest. For example, injury to Canada's diplomatic relations or short-term economic interests.
- SECRET: Applies to information or assets that, if compromised, could cause serious injury to the national interest. For example, serious injury to critical infrastructure or intelligence operations.
- TOP SECRET: Applies to information or assets that, if compromised, could cause exceptionally grave injury to the national interest. For example, grave injury to the security of the Canadian Armed Forces, relations with like-minded governments or loss of life.

Control systems

A control system is an administrative framework that protects sensitive sources of intelligence (Classified Information) by setting standards for access, marking, handling and control of information derived from or related to the intelligence source. Information protected by control systems is also known as compartmented information.

UNCLASSIFIED//NON CLASSIFIÉ

For example, the Special Intelligence (SI) is the control system that limits access to Signals Intelligence (SIGINT) and is intended to limit access to this information to those who are authorized to receive SI. SI Information requires special handling protocols. The SI control system has two further sub-control systems: GAMMA and Exceptionally Controlled Information (ECI), to impose additional limits on access to especially sensitive information.

- GAMMA: this system and its corresponding sub-compartments protect especially sensitive SIGINT reporting and related information.
- ECI: this system is comprised of multiple programs: each ECI program and its corresponding sub-compartments protect information related to an especially sensitive capability, method, or technique.
- Access to GAMMA or ECI information requires additional indoctrinations specific to that control system and compartment.

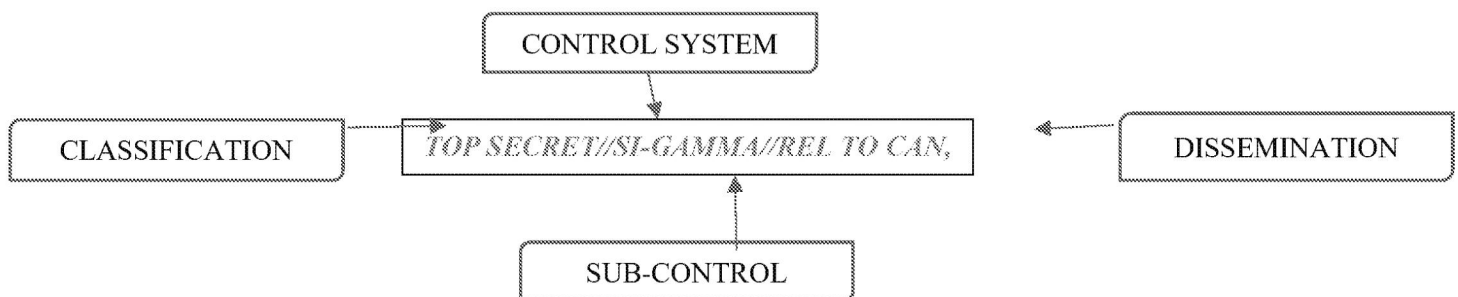
These control systems require special handling protocols, and even those with Top Secret clearance may not be indoctrinated to permit them to access all compartmented levels. Steps must therefore be taken to ensure that individuals have appropriate clearance, indoctrination, and need-to-know before information is shared, even within the S&I community.

Indoctrinations

As previously noted, not all those with Top Secret security clearances will have indoctrinations that permit them to access any or all compartmented information. Individuals are indoctrinated into a control system or sub-control system based on their need-to-know the information. Most control systems engage the framework under the *Security of Information Act* for special operational information and access requires TS clearance and ‘permanently bound to secrecy’ status (further described below).

Dissemination control

Dissemination control markings are used to limit the distribution of classified information to specific individuals, groups or nationalities, such as limiting dissemination of intelligence to *CANADIAN EYES ONLY (CEO)*, in accordance with their “Need-to-Know” and their level of security clearance.



Security of Information Act

The *Security of Information Act* (SOIA) is an Act of the Parliament of Canada that criminalizes the sharing of the most operationally sensitive government information. Certain departments, certain classes of people (past and current employees), and certain designated individuals who, by virtue of their position, would have access to “special operational information” are permanently bound to secrecy under SOIA. These are individuals who are held to a higher level of accountability for unauthorized disclosures of information obtained in relation to their work. For example, Military Intelligence, employees of CSIS and CSE, and certain members of the RCMP. The Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions is also permanently bound to secrecy.

Declassification And Sanitization

- Sanitization or Downgrading is the process to lower the classification of intelligence. For example, a document that had an original classification of TOP SECRET//SI//CEO may be sanitized to SECRET//CEO, if the information contributing to the TOP SECRET classification and SI control system is removed.
- Declassification is the process of making classified information unclassified. Generally this means removing or changing all information that could, if disclosed publicly, cause injury to the national interest, for example, by providing an adversary with the sources and methods of acquisition of the information.

The originating agency of the intelligence is the authority for sanitizing or declassifying intelligence. If the intelligence produced includes information obtained by a domestic partner agency or an international partner, then the originating agency must consult that partner on the sanitization or declassification of their information, and must obtain the approval of that partner to do so. In determining whether to sanitize or declassify information, the originating agency has to weigh the public interest in making the information available against the risk and costs associated with disclosing the information.

4) Protecting information: privileges and immunities

(4) An explanation of the various privileges and immunities that could apply to documents produced by the Government of Canada to the Commission over the course of its work;

Injury to National Security and the need for protection

Secrecy is essential for intelligence. For intelligence agencies to operate effectively, the knowledge, sources and methods used to obtain the information, and extent of the information they collect must remain confidential. This protects the integrity of past, present and future investigations, methodologies and capabilities of our intelligence agencies. Although agencies may acquire information from a variety of sources, in many circumstances this collection is conducted covertly, and as a result, the methods and sources of that collection cannot be disclosed.

As nations rely more heavily on interconnected digital systems and information networks, the vulnerability of sensitive data and information has increased exponentially. The injury to Canada of unlawfully disclosed intelligence information is significant. When this information is disclosed outside of authorized channels, it can have dire consequences: compromising national security operations, or exposing human or technical sources and methods, which can potentially endanger the lives of individuals involved (including consumers of that intelligence). There is also the risk

UNCLASSIFIED// NON CLASSIFIÉ

of losing access to technical sources of information, which are very expensive for Canada to obtain and maintain. Further, there is a risk to the trust and cooperation Canada enjoys with its closest partners and allies, such as the Five Eyes. This would undermine national security, Canada's global position, and pose risks to Canada's geo-political and economic stability.

The unauthorized disclosure of operational knowledge at a particular point in time, the specific operational assessment made by the agency, or the fact that the agency is in a position to draw certain conclusions regarding a subject or target, could indicate the level of interest, or lack thereof, in an individual or group at various points in time and the fact that the agency has enough information to make an assessment or draw a conclusion. Unauthorized disclosure of protected information could also:

- permit a subject of interest to deliberately introduce false or misleading information into an investigation if they become aware that they are under investigation;
- affect the scope and reliability of information available, as it would be unknown whether the information was false or misleading information; and
- enable the use of countermeasures by subjects of an investigation or operational targets against future investigative activities, which would lead to a gap in intelligence related to the threat.

On December 15, 2023, Canada provided the Commission a letter, which further explains injuries to international relations, national defence, and national security. This letter can be found at **Tab A**.

Privileges and Immunities

The Rules of Practice and Procedure provide that documents produced to the Commission by Participants may be subject to applicable privileges and immunities. While other privileges and immunities may also apply¹, the following two are particularly referenced:

- Section 37 of the *Canada Evidence Act*: Specified Public Interest Immunity (“SPII”)
- Section 38 of the *Canada Evidence Act*: International Relations, National Defence or National Security Privilege (“National Security Confidentiality” or “NSC”)

The Canada Evidence Act (“CEA”)

Section 37 of the CEA protects from disclosure information subject to SPII. The CEA does not define a “specified public interest”; it must be assessed on a case-by-case basis. The types of information often protected by SPII includes information that would identify a confidential informant; information related to on-going criminal investigations; information required to be protected in order to ensure the safety of officers, witnesses, victims and employees; sensitive police investigative techniques and information; internal police communications and intelligence; and organizational resourcing and structure in certain operational settings.

Section 38 protects from disclosure information that would be injurious to international relations, national defence or national security were it to be disclosed. See below for more details on NSC.

¹ Such as solicitor-client privilege, cabinet confidence, and litigation privilege

UNCLASSIFIED// NON CLASSIFIÉ

Section 39 protects from disclosure information that is covered by Cabinet Confidence. Section 39 of the CEA states that certification of information as Cabinet Confidence will protect that information without further examination or hearing of the information.

Section 38 of the CEA (NSC)

Section 38 CEA creates a process intended to deal with the protection of information, in the course of proceedings, the disclosure of which would injure international relations, national defence, or national security. Individuals involved in proceedings where there is the possibility that information of this type may be disclosed must provide notice to the Attorney General of Canada (AGC). This notice will permit the AGC to make a determination whether or not to authorize the disclosure of the information. If the AGC does not authorize disclosure of any of the information, or authorizes disclosure of only part of the information, judicial recourse is available through the Federal Court of Canada.

In practical terms, information that may be protected under NSC includes information that reveals or tends to reveal:

- the identity of a confidential source of information, except for CSIS human sources;
- targets of investigation;
- technical sources of information;
- methods of operation / investigative techniques;
- the identity of covert employees;
- telecommunications and cipher systems (cryptology);
- confidential relationship with a foreign government / agency, and information they have shared in confidence;
- confidential diplomatic exchanges;
- criticisms of a foreign government that would cause injury to international relations;
- information disclosing the strategies and objectives of the Canadian government in foreign affairs matters;
- consular information referring to a specific target of a national security investigation;
- characteristics, capabilities, performance, potential deployment, and functions or roles of Canadian Forces;
- military operations and policies relating to the conduct of military operations;
- intelligence operations, organizations and sources; and
- military equipment and telecommunications systems.

While the security classification of a document may be an indication that its disclosure could harm international relations, national defence, or national security, the classification itself is not determinative of these issues.

Statutory Disclosure Restrictions

Statutory disclosure restrictions that may apply to the information provided to the Commission could include:

- Court ordered publication bans;
 - *Criminal Code*: Section 164, Subsections 278.1 and 278.9, Section 320, Section 486.4, Section 486.5, Section 487.2, Section 517, Subsections 520(9), Section 539, Subsection 542(2), Subsection 631(6), Section 672.501
 - Provincial legislation (e.g. Subsection 137(2) of Ontario's *Courts of Justice Act*)
- Sealed warrants;
 - Section 487.3 of the *Criminal Code*;
- Wiretap authorizations;
 - Sections 187 and 193 of the *Criminal Code*;
- *Access to Information Act*;
 - Subsections 13(1), 15(1), and Sections 16, 17 and 19;
- *Criminal Records Act*;
 - Subsection 6(2), Section 6.1;
- *Privacy Act*;
 - Sections 7, 8(1), and 22;
- *Security of Information Act*, ss. 4 and 14;
- *Statistics Canada Act*, s. 17;
- *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*
 - sections 55(1) and 59(1)
- *Canadian Security Intelligence Service Act (CSIS Act)*
 - Sections 18(1) and 18.1
- *Communications Security Establishment Act (CSE Act)*
 - Section 55

Sections 18(1) and 18.1 of the CSIS Act

The CSIS Act prohibits the disclosure of information from which the identity of a CSIS employee that may become or has been engaged in covert operational activity may be inferred. The CSIS Act also prohibits the disclosure, in a proceeding, of the identity of a human source or any information from which the identity of a human source could be inferred.

Section 55 of the CSE Act

The CSE Act prohibits the disclosure, in a proceeding, of the identity of a person or entity that has assisted or is assisting CSE on a confidential basis, or any information from which the identity of such a person or entity could be inferred.

5) Protecting information: redactions and challenges

(5) An explanation of the internal process undertaken by the Government of Canada when responding to a request from the Commission that a document be publicly disclosed, including:

a. The internal process for determining whether information should be redacted on the basis of an applicable privilege or immunity, including a description of the positions/roles of those responsible for the analysis and the final decisions; and

b. The internal process undertaken when the Commission questions or challenges a redaction, including a description of the positions/roles of those responsible for the positions taken by the Government and for the interactions with the Commission.

Internal Litigation Team Process for determining whether information should be redacted, including Positions of those Responsible

Prior to documents being produced to the Commission, they are reviewed and redacted for Solicitor-Client Privilege, Cabinet Confidence and Litigation Privilege, with the stipulation that Canada does not waive any other applicable privilege, immunity or statutory disclosure restriction. This is done to facilitate the timely production of documents to the Commission.

When the Commission makes a request that documents be publicly disclosed or advises that they will be used in some part of the Commission's process, the documents identified by Commission Counsel will be reviewed by the litigation team to determine the owner of each document (ie. which Canadian department/agency produced or first received it). Departments/Agencies will be asked to advise the litigation team of all redactions that their department/agency may need to make on these documents prior to public disclosure. The litigation team will also ask departments/agencies to advise if, during their review, they become aware of any additional departments/agencies whose information may be contained within the documents in question. Each department/agency will provide their proposed redactions to the litigation team, identifying the basis for each.

Once these proposed redactions have been electronically applied to the documents by the litigation team, the litigation team will send that department/agency all documents with redactions made by that department/agency, with all their redactions identified by see-through highlights. The department/agency will be asked to confirm the proper application of redactions to their information (the "colour sign-off").

The start of the process is slightly different for CSIS documents. Given the specific sensitivities related to the CSIS information in question, as well as the efficiency achieved in reducing duplication of review, the litigation team will first send all CSIS-owned documents to CSIS for review. Once CSIS' redactions are finalized, and the colour sign-off has concluded, the CSIS-claimed information will be redacted from view (turned to black redactions), and these documents will then be sent to other departments/agencies for their review. All other departments/agencies will provide their proposed redactions to the litigation team on the CSIS documents. Each department's/agency's redactions will then be subject of a colour sign-off by that department/agency.

Once all department/agency-specific colour sign-offs are complete, a redacted version of the documents will be prepared. This version is intended to represent the documents as they would appear if made public. Each department and agency involved in the process will be invited to review the redacted version to ensure that no injurious information remains unprotected. Once

UNCLASSIFIED// NON CLASSIFIÉ

signoffs are received from all departments and agencies, the documents will be prepared for production to the Commission. This process takes considerable time and resources.

As the redaction process proceeds, all changes to redactions will be tracked electronically by the AGC's document management system.

The time required for departments/agencies and the litigation team to fulfil their review and document production role will depend on factors such as the nature, complexity, total number and length of the documents to be reviewed. The review for required NSC and SPII redactions involves the systematic review of every word in every document often many times over, to ensure accuracy and consistency. For example CSIS conducts an analysis to determine the source of information found in the document, the sensitivity of the source, whether it is partner information or not, analysis of CSIS public statements, and conducts an internal challenge function. This review can only be conducted by a limited number of individuals who possess the necessary security clearances and have familiarity with the injuries that would result from disclosure. The amount of time required is also affected by the requirement that those involved follow specific rules and procedures in relation to such documents.

Internal Department/Agency Process for determining whether information should be redacted, including Positions of those responsible

Usually, a core group of individuals is responsible for the redaction review process. These individuals are normally subject matter experts. Subject matter experts are individuals who have specialized factual knowledge and contextual background knowledge in relation to the issues raised in a particular proceeding. Those responsible for review within a department or agency identify proposed redactions specific to the interests of that particular department or agency and explain the rationale for protecting the information. Within a department or agency a proposed set of documents for production is generally reviewed multiple times by different client representatives (both to ensure review by those with different expertise, as well as to ensure quality control) and may also be reviewed by Departmental Legal Services Unit (DLSU) counsel. For example, within the RCMP, redactions are first proposed by analysts. These proposed redactions are then reviewed by one set of subject matter experts and then once more by another subject matter expert before the documents are reviewed by DLSU counsel. Once the internal review process is completed, the proposed redactions are sent to litigation counsel. In addition to discussions with litigation counsel, S&I community departments and agencies may consult with each other in relation to potential NSC and SPII redactions.

Internal Process When Commission Questions/Challenges a Redaction, including Positions of those Responsible

When the Commission questions or challenges a redaction, the following process will be followed:

- The challenge will be routed by litigation counsel to the appropriate department/agency.
- The department/agency will determine at a working level (i.e., subject matter expert) what advice will be provided to the responsible Assistant Deputy Minister or equivalent (ADM) regarding injury and the requirement for redaction. The department/agency may suggest an alternate method of making this information public, such as a summary. Other departments/agencies will be consulted at this stage if necessary. The department/agency may need to conduct further research or consultation in order to properly address the challenge.

UNCLASSIFIED// NON CLASSIFIÉ

- The advice will then be briefed up to the ADM for approval. The ADM will determine whether any redaction can be lifted at this stage (perhaps a redaction was made in error, or the injury analysis assessed too high a risk). The ADM could also decide to brief up to the Deputy Minister or equivalent (DM) level. If a decision is made at the ADM level, the litigation team will be advised at this stage.
- If raised to the DM, the DM will make a decision based on the ADM's recommendation, any legal advice, and any information received from other agencies. The DM's decision would be communicated to the litigation team at this stage.
- The litigation team will perform a challenge function throughout the department/agency decision-making process, involving the National Security Group at the Department of Justice as needed.
- The final decision on all Commission challenges will remain with the DM of the department/agency in question, and will be communicated to the Commission via litigation counsel.
- If the Commissioner disputes the decision made, recourse may be had to the relevant court in accordance with applicable laws. In relation to information that the Commissioner concludes would not be injurious to the critical interests of Canada or its allies, national defence or national security and so notifies the AGC, in accordance with the Terms of Reference, this will constitute notice under section 38 of the CEA. The AGC will then make a decision with respect to the disclosure of the information. Following this decision, further recourse is available through the Federal Court, if required, in accordance with section 38.04.

UNCLASSIFIED// NON CLASSIFIÉ

TAB A – December 15, 2023 letter from Canada to Commission Counsel



**Department of Justice
Canada**

National Capital Region
National Litigation Sector
50 O'Connor Street, Suite 500
Ottawa, ON K1A 0H8

**Ministère de la Justice
Canada**

Région de la Capitale nationale
Secteur national du contentieux
50, rue O'Connor, bureau 500
Ottawa (ON) K1A 0H8

VIA EMAIL

**UNCLASSIFIED LETTER
WITH TOP SECRET ATTACHMENTS**

December 15, 2023

**To: Shantona Chaudhury
Lead Commission Counsel
Public Inquiry into Foreign Interference in
Federal Electoral Process and Democratic
Institute**

Dear Ms. Chaudhury:

Re: National Security Confidentiality Review of 13 Selected Documents

The Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (Inquiry) was established in September 2023 following the concurrence of the Government of Canada, the leaders of all recognized parties in the House of Commons, and the Honourable Madam Justice Marie-Josée Hogue on the proposed Terms of Reference.

Upon appointment, the Commissioner was provided an opportunity to review certain information related to the work of the Inquiry. The Inquiry has asked the Government of Canada to review a selection of those documents (the selected documents) to which the Inquiry has access for the purpose of assessing what these documents would look like if used publicly.

The Government has concluded this exercise, and the instant correspondence contains a response in six components: (i) this letter; (ii) the selected documents, redacted as necessary to permit their public disclosure; (iii) the selected documents with see-through highlights which identify the rationale for each redaction; (iv) a classified Annex providing additional information as to the injury that would result from disclosure; (v) a coding guide which identifies the injury associated with each redaction; and (vi) summaries of three Canadian Security Intelligence Service (CSIS) Intelligence Reports from the selected documents prepared for discussion purposes (see below in relation to options going forward). Items (i) and (ii) are unclassified, and the Government consents

to their public disclosure. Items (iii), (iv), (v), and (vi) are classified and cannot be disclosed publicly.

The documents at issue demonstrate in concrete terms one of the most difficult practical constraints that the Inquiry will face in fulfilling its mandate. While public hearings on the challenges, limitations and potential adverse impacts associated with the disclosure of national security information and intelligence to the public are envisioned by paragraph (a)(i)(D) of the Inquiry's Terms of Reference, the current exercise highlights several of the applicable considerations. The Government has proposed certain tools for the Inquiry's consideration, and invites a discussion on these matters at the Inquiry's convenience.

Terms related to Classified, Sensitive and Injurious Information

In particular, it is helpful to clarify, in general terms, certain definitions that apply in respect of the Inquiry's work.

First, the term "classified information" applies to information the unauthorized disclosure of which could reasonably be expected to cause injury to the national interest. Classified information can be categorized as "Confidential", "Secret" and "Top Secret". By way of illustration, the classification "Top Secret" applies to information when unauthorized disclosure could reasonably be expected to cause *exceptionally grave injury* to the national interest.

Similarly, the term "compartmented information" refers to information derived from sensitive sources and methods. Access to compartmented information is limited to Top Secret cleared Canadian citizens who are authorized to access the information after receiving a formal indoctrination. Compartments are implemented by controlling access to information using frameworks known as control systems. Control systems define who may access the information, and under what conditions. Much of this information is also "special operational information" under the *Security of Information Act*.

In addition to these classifications, "sensitive information" is information relating to international relations or national defence or national security that the Government of Canada is taking measures to safeguard. In turn, "injurious information" is information that if it were disclosed to the public, would injure Canada's international relations or national defence or national security.

While various Government policies exist for the protection of classified information, Parliament has established a comprehensive regime for the protection of sensitive and injurious information, found in section 38 of the *Canada Evidence Act*, and adjudicated by the Federal Court of Canada. The Inquiry is bound by these restrictions, and others, in accordance with paragraphs (a)(iii)(E) and (a)(iv) of the Terms of Reference, which include a requirement to protect human sources pursuant to section 18.1 of the *Canadian Security Intelligence Service Act*.

Explaining Injury

The selected documents were drafted for a limited audience of individuals holding the required security clearance. As a result, the documents include a significant amount of highly classified,

sensitive, and injurious information that cannot be disclosed and that must be carefully safeguarded. The result is that a significant proportion of that information could not be released publicly under any circumstance without causing injury to Canada's national security, national defence, or international relations.

By way of illustration, when the Government asserts that disclosure would be injurious to national security, national defence, or international relations, this can mean more specifically that, among other things:

- With respect to *national security*, disclosure would undermine ongoing or future national security operations or investigations, endanger individuals who work or cooperate with the Government's departments and agencies, and enable threat actors to engage in counter-measures. For instance, disclosure may reveal, directly or indirectly:
 - o Interest in individuals, groups or issues, including the existence or non-existence of past or present files or investigations, the intensity of investigations, or the degree or lack of success of investigations;
 - o Methods of operation and investigative techniques;
 - o Relationships with other police, security and intelligence agencies and the information exchanged in confidence with such agencies;
 - o Employees, internal procedures, administrative methodologies, and telecommunications systems; and
 - o Persons who cooperate with or provide information in confidence to Canadian intelligence agencies.

- With respect to *international relations*, disclosure would undermine Canada's relationship with important allies. This includes the exchange of information between foreign nations and the ability to conduct such exchanges in an atmosphere of trust to ensure the information is as complete and accurate as possible. Releasing such information would compromise or impair the trust of not only the nation to whom it relates, but of other foreign nations as well. Canada benefits tremendously from these exchanges and it must maintain the trust of all foreign nations to continue to benefit from those. Closely related, the "third party rule" is an understanding among information-sharing partners that information providers maintain control over subsequent disclosure and use. A breach of the third party rule would likely have a negative impact on the parties' relations, the most likely of which would be a cessation or reduction of future information sharing.

In reviewing the selected documents, the Government scrutinized the information at issue, and devoted significant resources to determining the scope of injury that could arise from the public disclosure of that information. The Government would, if necessary, object to any further disclosure of the information contained in the sample documents pursuant to section 38 of the *Canada Evidence Act* were the Inquiry to insist on its public disclosure.

The majority of the selected documents are CSIS documents. Redactions are made within these documents by CSIS, the Communications Security Establishment, Global Affairs Canada, the Royal Canadian Mounted Police, and the Financial Transactions and Reporting Analysis Center of Canada. We note that the result of the exercise is that the CSIS documents are redacted almost in their entirety. Given that the majority of the redactions made within the selected documents are linked to CSIS information, this letter focuses on CSIS information.

CSIS Intelligence

The CSIS documents in question are CSIS products meant to disseminate intelligence to a government readership for use in their own analysis and to inform the decision-making, specific to their department. The documents range from single pieces of intelligence, to comprehensive analytical products that are based on multiple reporting streams, both domestic and foreign. One important commonality among the documents is that they are written solely for a readership that has the appropriate security clearance to access and use the intelligence in question.

CSIS intelligence is not classified and restricted to a small readership because it is intelligence, in and of itself, or simply because it is derived from classified sources. Rather, a security classification and restricted distribution is applied because the release of the intelligence will expose a human or technical source, a methodology, an investigation or investigative gap to adversaries or it will cause harm to international relationships. This is certainly true with respect to intelligence regarding the threat-related activities of foreign governments that have considerable resources at their disposal to conduct counter-intelligence investigations.

Intelligence concerning multiple aspects of the People's Republic of China (PRC) Foreign Interference and Malign Influence activities are of the utmost importance for the government of Canada because of the scope and impact of this threat. These activities involve immediate threats or grave harm to Canada's strategic interests. These are activities on which the Government needs to be fully and comprehensively informed in order to make immediate and effective policy or operational decisions. These activities address those issues which have the highest importance for Canadian interests, carry the highest potential to negatively or positively impact Canadian interests, and have the highest need for distinctly Canadian intelligence insights.

Foreign Interference

The threat of foreign interference in our democratic processes emanates from the PRC and other countries. The public release of Canada's intelligence, particularly *as these products are currently written*, risks exposing CSIS sources, and the extent to which Canada understands, or lacks understanding, of threat activities. This is compounded by the mosaic effect, wherein an adversary tracks and pieces together a large number of individual, possibly disparate, pieces of intelligence, often gathered over long periods of time, from multiple sources, and thereby gains the ability to piece together a picture of our holdings. It may not always be possible to point to a specific piece of information in an individual document and explain why its release would be injurious in and of itself, but when combined with other publicly released information, or that which has been acquired through espionage and data theft, adversaries may be able to draw inferences and

conclusions regarding CSIS's investigations. That which may be exposed through this effect, and is of high interest to the foreign intelligence services that are active in Canada include investigative interests, intelligence gaps, methods of operation, administrative procedures, employees, foreign partnerships, locations of technical sources and, the identity of CSIS' casual contacts and human sources.

Foreign state actors engaged in foreign interference have significant capabilities to aggregate "big data" and utilize geolocation information and artificial intelligence to piece together information from a variety of different products or reporting streams that have been released over a number of years. For example, media reporting has indicated that the PRC has previously successfully used such capabilities to dismantle the CIA's human source network, resulting in severe consequences, including imprisonment and dozens of lives lost.¹

The classified Annex attached to this letter uses a specific example from the selected documents to explain the specifics of why it would be injurious to Canada's national security to release that information.

It is also vital to note that foreign interference investigations, like foreign interference itself, often continue over years or decades. Many access points of Canadian intelligence on this issue take long periods of time to develop and remain in place for extended timeframes. Many of the foreign interference investigations that were active in 2019 and 2021, are active investigations today, meaning their exposure will negatively impact current on-going investigations. Critically, if they are in place, disclosures that identify human sources, or allow for their identities to be inferred, risk sources' safety, and the safety of those close to them.

Disclosure would also have longer term negative implications. It is reasonable to assume that foreign officials are following the Inquiry such that disclosure of sensitive information would become known to them. This will likely lead to an immediate loss of access to the intelligence that Canada has deemed to be of the highest priority. This access would take years to replicate and replace (if it could be replaced at all). Finally, such inability to protect human sources, and classified information in general, would likely result in decreased confidence in CSIS by other individuals considering providing information to CSIS, and foreign agency partners, potentially resulting in decreased intelligence received.

Resources

This national security confidentiality (NSC) review of the selected documents was conducted on an expedited basis. To meet the timeframe provided, the government diverted subject matter experts familiar with the specific intelligence contained in the documents from their intelligence collection and analysis roles in order to support the review. This is a deviation from their standard process. In total, personnel spent in excess of 200 person hours on the review of these 13 documents. As you may be aware, the government takes the review process seriously as it can have collateral consequences on other investigations and proceedings, including court

¹ *China Used Stolen Data to Expose CIA Operatives in Africa and Europe*, foreignpolicy.com

- 6 -

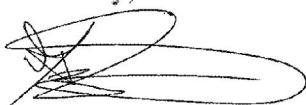
proceedings. The government typically sources all statements made in intelligence work products back to the raw intelligence to confirm, among other things, accuracy of the report and the method of collection. This level of NSC review is not sustainable if replicated over a longer term. It is clear that redactions of documents on a large scale will not be a productive way forward within the timeframe allotted.

Other Options for the Way Forward

The Government of Canada recognizes the importance of educating the public on the threat of Foreign Interference. In doing so it is vital to protect information that would be injurious to national security if released. We are committed to assisting the Inquiry in achieving its mandate. In that regard we would like to open a dialogue on viable options to help meet the Commissioner's mandate. Part of that dialogue requires a better sense of what type of information the Inquiry is interested in making public, with the understanding that there are very practical limitations on what classified information can be made public. With this in mind, we believe that the following options and/or a combination of these options will help further this process. These options include redactions on a limited number of documents that is sustainable and proportionate, summaries of a limited number of documents or topics (see examples in classified attachments), and/or *ex parte in camera* hearings leading to a public summary.

We are available to meet at your convenience but would like to open this dialogue as soon as possible.

Yours truly,



Greg Tzemenakis, Senior General Counsel
Barney Brucker, A/Senior General Counsel
National Litigation Sector

Encls. 13 Selected Documents, redacted (Unclassified)
13 Selected Documents, highlighted (Classified)
Annex (Classified)
Coding Guide (Classified)
3 Summaries (Classified)

Canada