

For Public Release



Public Safety Canada / Sécurité publique Canada

### Routing Slip / Bordereau d'acheminement

Branch / Secteur: NCSB / SCN		Directorate / Direction générale: NSPD	
CCM File No / N° de dossier CCM: PS-040896		RDIMS Groups requiring access / Groupes du SGDDI requérant l'accès:	
RDIMS / SGDDI, GCDOCS, other / autre (all attachments / toutes les pièces jointes):		Docket Security Level / Niveau de sécurité de dossier:  Secret	Seeking Final Approval By Date / Obtenir l'approbation définitive d'ici le:  N/A

**Docket Title (English):**

**Implementation of Ministerial Direction to the Canadian Security Intelligence Service on Threats to**

**Titre du dossier (français):**

**Mise en œuvre des directives ministérielles sur les menaces à la sécurité du Canada dirigées**

Is the title releasable? / Le titre peut-il être publié? Yes / Oui	Reason for non release / Raison de non-publication :	Final Recipient / Destinataire final: Minister LeBlanc/Minister's Office
---	--	---

Routing / Acheminement	Date (yyyy/mm/dd) (aaaa/mm/jj)	Initials / Initiales	Action Required / Mesures à prendre	
			Approval or Signature / Approbation ou signature	For Information / Pour information (cc)
Originator / Auteur	2023/08/18	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Manager / Gestionnaire	2023/08/18	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Director / Directeur (Directrice)	2023/08/18	<input type="checkbox"/> for <input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Director General / Directeur général (Directrice générale) Lesley Soper	2023/08/18	<input type="checkbox"/> for LS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Chief Audit Executive / Dirigeant(e) principal(e) de la vérification Miranda Shepard			<input type="checkbox"/>	<input type="checkbox"/>
Chief Financial Officer and Assistant Deputy Minister, CMB / Dirigeant(e) principal(e) des finances et sous-ministre adjoint(e), SGM Patrick Amyot			<input type="checkbox"/>	<input type="checkbox"/>
Assistant Deputy Minister PACB / Sous-ministre adjoint(e) SAPC Shannon Grainger			<input type="checkbox"/>	<input type="checkbox"/>
Assistant Deputy Minister, CPB / Sous-ministre adjoint(e), SPC Tala Dakalbab			<input type="checkbox"/>	<input type="checkbox"/>
ADM Indigenous Affairs Branch / SMA, Direction des affaires autochtones Chris Moran			<input type="checkbox"/>	<input type="checkbox"/>
ADM Firearms Program Branch / SMA, Direction du programme des armes à feu Greg Kenney			<input type="checkbox"/>	<input type="checkbox"/>
Assistant Deputy Minister, EMPB / Sous-ministre adjoint(e), SGUP Trevor Bhupsingh			<input type="checkbox"/>	<input type="checkbox"/>
Senior Assistant Deputy Minister, NCSB / Sous-ministre adjoint(e) principal(e), SSCN Patrick Boucher		<i>Ag 22</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Associate Deputy Minister / Sous-ministre délégué(e) Tricia Geddes		<i>AB</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**REÇU AU BUREAU  
DU SM**

AUG 22 2023

**RECEIVED IN  
DM'S OFFICE**

RDIMS / SGDDI # 2714121



For Public Release



Public Safety / Sécurité publique  
Canada / Canada

**Routing Slip / Bordereau d'acheminement**

Deputy Minister / Sous-ministre Shawn Tupper			<input checked="" type="checkbox"/>	<input type="checkbox"/>
Minister of Public Safety / Ministre de la Sécurité publique The Honourable Dominic LeBlanc, PC, KC, MP			<input checked="" type="checkbox"/>	<input type="checkbox"/>
Minister of Emergency Preparedness / Ministre de la Protection civile The Honourable Harjit S. Sajjan, PC, OMM, MSM, CD, MP			<input type="checkbox"/>	<input type="checkbox"/>
<b>Consultations :</b>				
Group Name / Nom de groupe	CSIS			
Consulted during development of draft materials	<input checked="" type="checkbox"/> Yes / Oui	<input type="checkbox"/> Yes / Oui	<input type="checkbox"/> Yes / Oui	<input type="checkbox"/> Yes / Oui
Consulté au cours de l'élaboration des documents				
Incorporated feedback	<input checked="" type="checkbox"/> Yes / Oui	<input type="checkbox"/> Yes / Oui	<input type="checkbox"/> Yes / Oui	<input type="checkbox"/> Yes / Oui
Commentaires incorporés				
<b>Notes :</b>				

RDIMS / SGDDI #



For Public Release



Public Safety    Sécurité publique  
Canada            Canada

Deputy Minister    Sous-ministre

Ottawa, Canada  
K1A 0P8

**SECRET // CEO**

DATE: AUG 23 2023

File No.: NS 6210 / PS-040896

**MEMORANDUM FOR THE MINISTER OF PUBLIC SAFETY, DEMOCRATIC  
INSTITUTIONS AND INTERGOVERNMENTAL AFFAIRS**

**IMPLEMENTATION OF MINISTERIAL DIRECTION  
TO THE CANADIAN SECURITY INTELLIGENCE SERVICE  
ON THREATS TO PARLIAMENT AND PARLIAMENTARIANS**

(For Decision and Signature)

**ISSUE**

Your decision is sought on a governance protocol developed to support implementation of the Ministerial Direction to the Canadian Security Intelligence Service (CSIS) on threats to the security of Canada directed at Parliament and parliamentarians, as issued by your predecessor on May 16, 2023 (**TAB A**). Following issuance of the Direction, Public Safety Canada (PS) has worked with CSIS to elaborate this protocol in order to facilitate internal government coordination to support the Minister of Public Safety's expectation that CSIS will seek, wherever possible, to ensure that parliamentarians are informed of the threats to the security of Canada directed at them.

**BACKGROUND**

The Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians established expectations that:

- CSIS will investigate threats to the security of Canada directed at Parliament and parliamentarians in a manner proportional to the threat and the importance of the institution to Canada's democracy;
- CSIS will pursue the appropriate lawful methods to respond to threats to the security of Canada directed at Parliament and parliamentarians, including the taking of threat reduction measures and disclosing information to the Royal Canadian Mounted Police or other law enforcement body; and,

For Public Release

**SECRET // CEO**

- 2 -

- CSIS will seek, wherever possible within the law and while protecting the security of its operations, to ensure that parliamentarians are informed of threat activities directed towards them.

The Direction also requires CSIS to inform the Minister of Public Safety of all instances of threats to the security of Canada directed at Parliament and parliamentarians. When it does so, CSIS is expected to explain how its response addresses the three expectations outlined above.

The Ministerial Direction applies whenever CSIS assesses a threat to the security of Canada is being directed at Parliament or a parliamentarian. The Direction is not triggered by the mere existence of threatening behaviour or communications that mention or implicate a parliamentarian. Under the Ministerial Direction, CSIS's first obligation is to investigate potential threats and assess whether there is a threat to the security of Canada.

(TAB C). As a next step, and consistent with the Ministerial Direction, CSIS will investigate further to verify the information and assess the nature of the potential threat to the security of Canada.

In general terms, CSIS assesses that a threat exists based on the totality of information available to it, including all available information on the threat, capabilities and intentions of the threat actor, and taking into account the credibility and specificity of the available information. This function involves the application of judgement, professional practice, and expertise, and is rooted in CSIS's mandate as an intelligence collector and assessor applying the definition of threats to the security of Canada established by the *CSIS Act*.

Once CSIS has assessed a threat to the security of Canada is being directed at Parliament or a parliamentarian, then its obligations to pursue the appropriate lawful response and inform the parliamentarian, wherever possible, apply.

There are several ways in which CSIS may brief parliamentarians on threats to the security of Canada directed at them. These include unclassified "defensive briefs" and threat reduction measures that involve the disclosure of intelligence. In addition, scenarios may arise in which CSIS would be disclosing information in order to further its investigative needs (often referred to as "give to get").

### **CONSIDERATIONS**

Disclosures of information derived from intelligence raise a number of important policy and operational considerations that must be carefully taken into account when considering disclosures. These include:

For Public Release

**SECRET // CEO**

- 3 -

- *Effectiveness and lawfulness:* Some options for briefing the parliamentarian may not be available due to legal limitations. Wherever possible, the approach that will best contribute to the parliamentarian's security should be preferred.
- *Operational security and effectiveness:* Disclosures of information could introduce a risk to CSIS's operational security, including the safety of sources and the effectiveness of intelligence collection methods.
- *Creation of liabilities:* Once information is disclosed, the federal government does not have control over how the recipient will use the information. If subsequent action is unreasonable (e.g., dismissal of an employee), it could create a real or perceived liability for the federal government for its part in the recipient's actions.
- *Deconfliction with law enforcement investigations:* It is imperative that the judicial system remains the primary avenue for addressing domestic conduct that harms Canada or Canadians. Disclosures of intelligence that are not properly coordinated and consulted with law enforcement can disrupt their investigations and impair charges and prosecution.
- *Maintaining CSIS's objectivity:* To maintain CSIS's effectiveness, it is important that it is regarded as an impartial and nonpartisan actor. Disclosures of information, particularly in the parliamentary space, could risk creating the perception that these disclosures are related to political discussions and deliberations.

It is also important that government officials act in a timely and coordinated manner with respect to Parliament, and that Ministers have appropriate awareness of the actions being taken within this core political body.

### **PROTOCOL**

PS has worked with CSIS and other implicated departments and agencies to develop a governance protocol for threat disclosures to parliamentarians. The protocol lays out a sequential process for consulting and coordinating proposed disclosures within government to allow the above considerations to be fully addressed in the approach to briefing parliamentarians. These steps complement the requirements in the Ministerial Directions on Operations and Accountability to review operational activities for risk, which ensure appropriate consultation with the Department of Justice and Global Affairs Canada. Pursuant to the Ministerial Direction for Operations, if CSIS plans to undertake a threat reduction measure that attracts a high risk under any of the four pillars, your approval will also be sought.

### **APPROVAL**

PS and CSIS are seeking your approval of this protocol to provide formal confirmation that you agree with the approach it outlines. Normally, operational procedures at this level of detail would

For Public Release

**SECRET // CEO**

- 4 -

not be subject to your approval, as the Director of CSIS is responsible for control and management of the Service as well as matters such as assessing intelligence to form judgements, consulting with other departments, and assessing risks.

In this case, PS and CSIS want to ensure you agree that the Ministerial Direction requirement to brief parliamentarians is subject to CSIS's investigation of potential threats and assessment that a threat exists based on the totality of the information available. The protocol also makes clear that threat activity is distinct from legitimate activities, such as foreign diplomacy.

As your approval would represent formal guidance on the implementation of the Ministerial Direction, it is recommended that you provide a copy of the protocol to the National Security Intelligence Review Agency (NSIRA), as must be done with a Ministerial Direction proper. This would ensure that NSIRA has a complete understanding of your general guidance to CSIS on this matter.

CSIS and PS intend to review this protocol and amend it as required based on experience and operational developments. If you decide to approve the document, PS and CSIS will return to seek approval of any substantive changes.

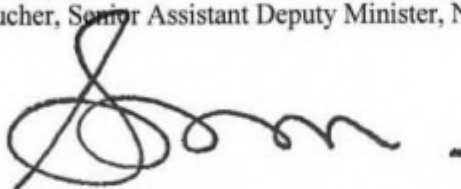
SECRET // CEO

- 5 -

RECOMMENDATION

It is recommended that you approve the governance protocol for CSIS threat disclosures to parliamentarians. It is also recommended that you sign a letter transmitting the protocol to NSIRA (**TAB D**), so that NSIRA has a record of your approval of internal guidance on the implementation of the Ministerial Direction.

Should you require additional information, please do not hesitate to contact me or Patrick Boucher, Senior Assistant Deputy Minister, National and Cyber Security, at 613-990-4976.



Shawn Tupper  
Deputy Minister

I concur

I do not concur

I concur with changes



The Honourable Dominic LeBlanc, P.C., K.C., M.P.

Date:

Sept. 19/23

Attachments (4):

Tab A: Ministerial Direction to the Canadian Security Intelligence Service (CSIS) on threats to the security of Canada directed at Parliament and parliamentarians

Tab B: Governance Protocol for Threat Disclosures To Parliamentarians

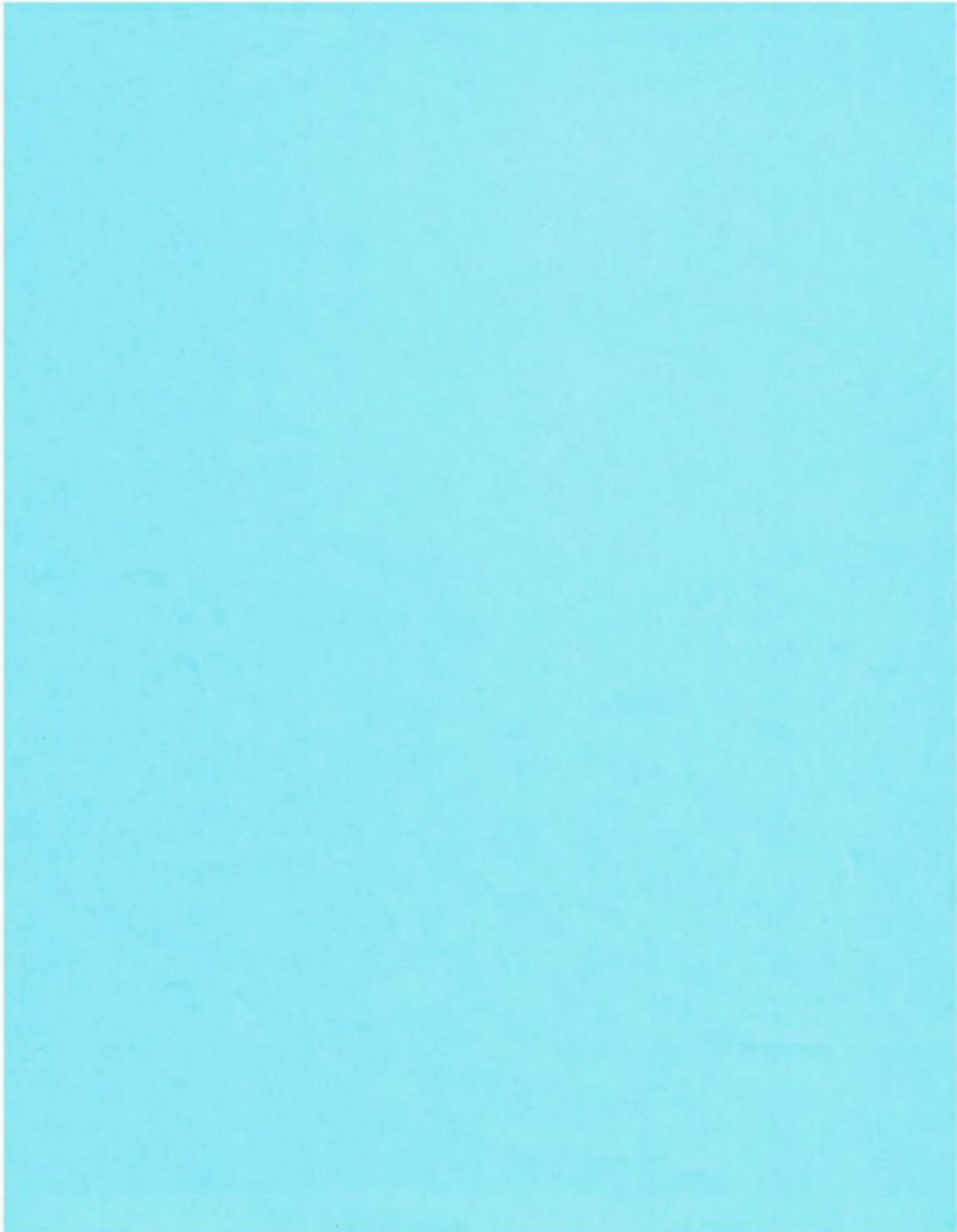
Tab C:

Tab D: Letter to Marie Deschamps, Chair, National Security and Intelligence Review Agency

Prepared by:  A/Manager, National Security Policy Directorate, National and Cyber Security Branch

Input provided by: CSIS

For Public Release





For Public Release

**MINISTERIAL DIRECTION ON THREATS TO THE SECURITY OF CANADA**  
**DIRECTED AT PARLIAMENT AND PARLIAMENTARIANS**

The Parliament of Canada is at the heart of Canada's democracy. As such, it is imperative that all parliamentarians are able to exercise their roles fully and without hindrance or interference from foreign states or hostile actors.

To this end, I expect that threats to the security of Canada directed at Parliament and parliamentarians, including those conducted through their family and staff, receive the highest level of attention from the Canadian Security Intelligence Service (CSIS) in collaboration with the national security and intelligence community. In doing so, I continue to expect that CSIS will at all times respect the *Canadian Charter of Rights and Freedoms* and the rule of law.

Pursuant to subsection 6(2) of the *Canadian Security Intelligence Service Act*, I have issued the following direction to describe my expectations in this regard.

1. CSIS will investigate all threats to the security of Canada that target Parliament and parliamentarians in a manner proportional to the threat and the importance of Parliament to Canada's democracy and national security.
2. When CSIS assesses, in accordance with its mandate, there to be a threat to the security of Canada directed at Parliament or a parliamentarian, it will pursue the appropriate lawful methods in response, including but not limited to the taking of threat reduction measures and disclosures to the Royal Canadian Mounted Police or other law enforcement agencies.
3. CSIS will seek, wherever possible within the law and while protecting the security and integrity of national security and intelligence operations and investigations, to ensure that parliamentarians are informed of threats to the security of Canada directed at them. This may involve direct disclosures, or by working with other bodies, such as Government of Canada departments, the Royal Canadian Mounted Police, or other law enforcement agencies, as the law permits.
4. The Minister of Public Safety will be informed of all instances of threats to the security of Canada directed at Parliament or parliamentarians in a timely manner and with an explanation of how CSIS will implement the above directions.

For Public Release



For Public Release

SECRET // CEO

MINISTERIAL DIRECTION ON THREATS TO THE SECURITY OF CANADA  
DIRECTED AT PARLIAMENT AND PARLIAMENTARIANS

---

**GOVERNANCE PROTOCOL FOR THREAT DISCLOSURES TO PARLIAMENTARIANS**

**Initiation and Application:**

- CSIS will initiate this protocol whenever it assesses that there exists a threat to the security of Canada directed at a parliamentarian and identifies that disclosure of information to the parliamentarian is possible within the law and while protecting the security and integrity of national security and intelligence operations and investigations. This includes disclosures conducted as threat reduction measures as well as under other authorities.
- CSIS will assess that a threat exists in accordance with its mandate, as established by the *CSIS Act*, including by applying the definition of threats to the security of Canada and fulfilling its role as an intelligence collector and assessor. These functions involve the application of judgement, professional practice, and expertise.
- As such, CSIS will assess that a threat exists per its operational procedures and practices for assessing intelligence. CSIS is expected to take into account all available information on the threat, capabilities and intentions of the threat actor, with due regard to whether the information is credible, corroborated, and particularized to the individual being briefed.
- Only information on a credible threat to the security of Canada directed at a parliamentarian that is differentiated from legitimate activities (lawful advocacy, protest, dissent, diplomatic activity) *may* be disclosed, unless the Service assesses that these activities are being carried on in conjunction with or in support of a suspected threat to the security of Canada.

**Protocol:**

**1. Threat Briefing Package:**

- **Intelligence package** of the information on the threat to national security directed at the parliamentarian, including published products and extracts from undisseminated intelligence.
- **Key messages** for the threat-specific briefing. This will be used by two CSIS officials to brief the MP on the intelligence.

**2. ADM Consultation:** CSIS will share the threat briefing package prior to a meeting of the ADM National Security Operations (Tactical) committee for discussion.

- In addition to CSIS, participants will include Public Safety Canada, the Privy Council Office, Global Affairs Canada, the RCMP, and any other implicated departments or agencies. The discussion will include consideration of the intelligence products and Key Messages. Any changes to the Key Messages that are requested must be provided in writing with appropriate accountabilities.

For Public Release

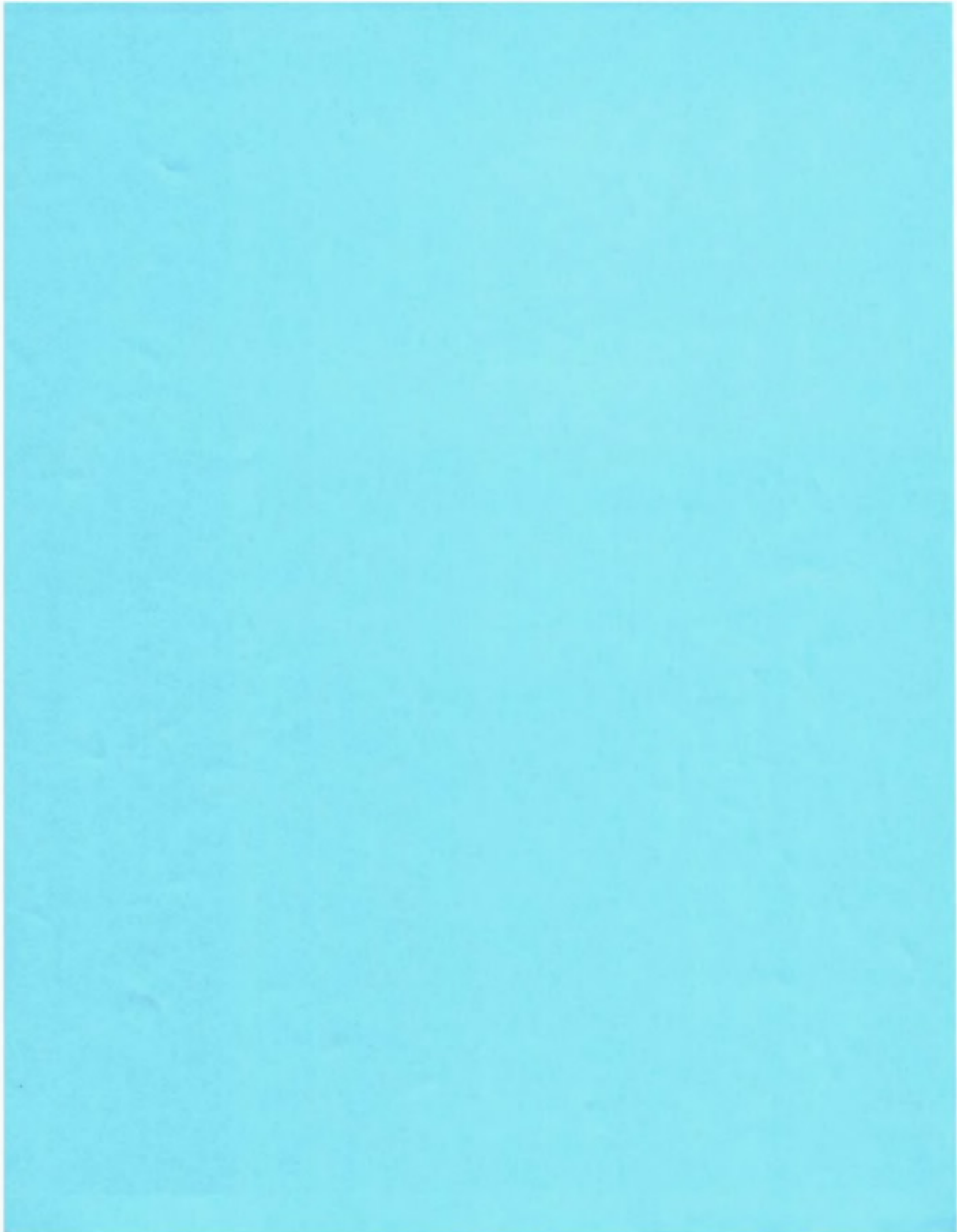
SECRET // CEO

3. ***DM Consultation:*** After the ADM consultation, CSIS will bring the threat briefing package – revised if necessary – to a meeting of the Deputy Ministers’ Committee on Intelligence Response. The purpose of this discussion is to provide advice to the Director of CSIS; the advice of DMs will be recorded in a record of discussion and any requested changes must be provided in writing. DMs will also decide on an approach to briefing Ministers.
4. ***CSIS Approvals of Operational Plan:*** CSIS will seek the necessary internal approvals for the operational activity (e.g. TRM or s. 12 interview). This will include conducting a four-pillar risk assessment, including consultations with Justice and, where there is a foreign policy component, Global Affairs Canada.
5. ***Briefing/Approval of Minister of Public Safety:*** CSIS will share the threat briefing package with the Minister of Public Safety. As per ministerial direction, if CSIS plans to undertake a threat reduction measure that attracts a high risk under any of the four pillars, the approval of the Minister of Public Safety will be sought.
  - The Deputy Minister of Public Safety will provide any advice that may be needed.
  - If recommended or requested, the Minister may receive a verbal briefing from CSIS and Public Safety Canada.
  - Responsive communications lines will be developed in consultation/coordination with partners as appropriate in the circumstances.
6. ***Brief Ministers:*** The threat briefing package will be shared with other Ministers, as directed by DMs. At its discretion, PCO will also brief the Prime Minister on the operational plan.
7. ***Conduct Operational Activity:*** CSIS will brief the parliamentarian, using the Key Messages and according to the appropriate authority. The briefing will be conducted by two officials from CSIS with subject matter experts to support as necessary.
8. ***Rapid Debrief:*** CSIS will provide a rapid read out via Issues Management Brief and disseminate it to the ADM NS OPS (Tactical) meeting participants and established points of contact. Additional ADM NS OPS or DM CIR meetings may be convened to coordinate ongoing issues management, if required.

**Record keeping:** Records of decision will be kept for all ADM and DM meetings as well as ministerial briefings where approval or direction is provided.

**Modification for conflicts of interest:** Public servants, exempt staff, and Ministers operate in and around Parliament. There is a risk that individuals involved in this process have an interest in the outcome. From time to time, adjustments to the protocol may be needed to limit distribution of a document or otherwise modify a step to avoid real or perceived conflicts of interest. If CSIS identifies such a concern, they will raise it with Public Safety Canada for agreement on the revised process for that specific instance.

For Public Release



For Public Release



# National Security Brief | Précis sur la sécurité nationale

[Redacted] (S//CEO)

[Large redacted area]

### Next Steps

[Redacted area under Next Steps]

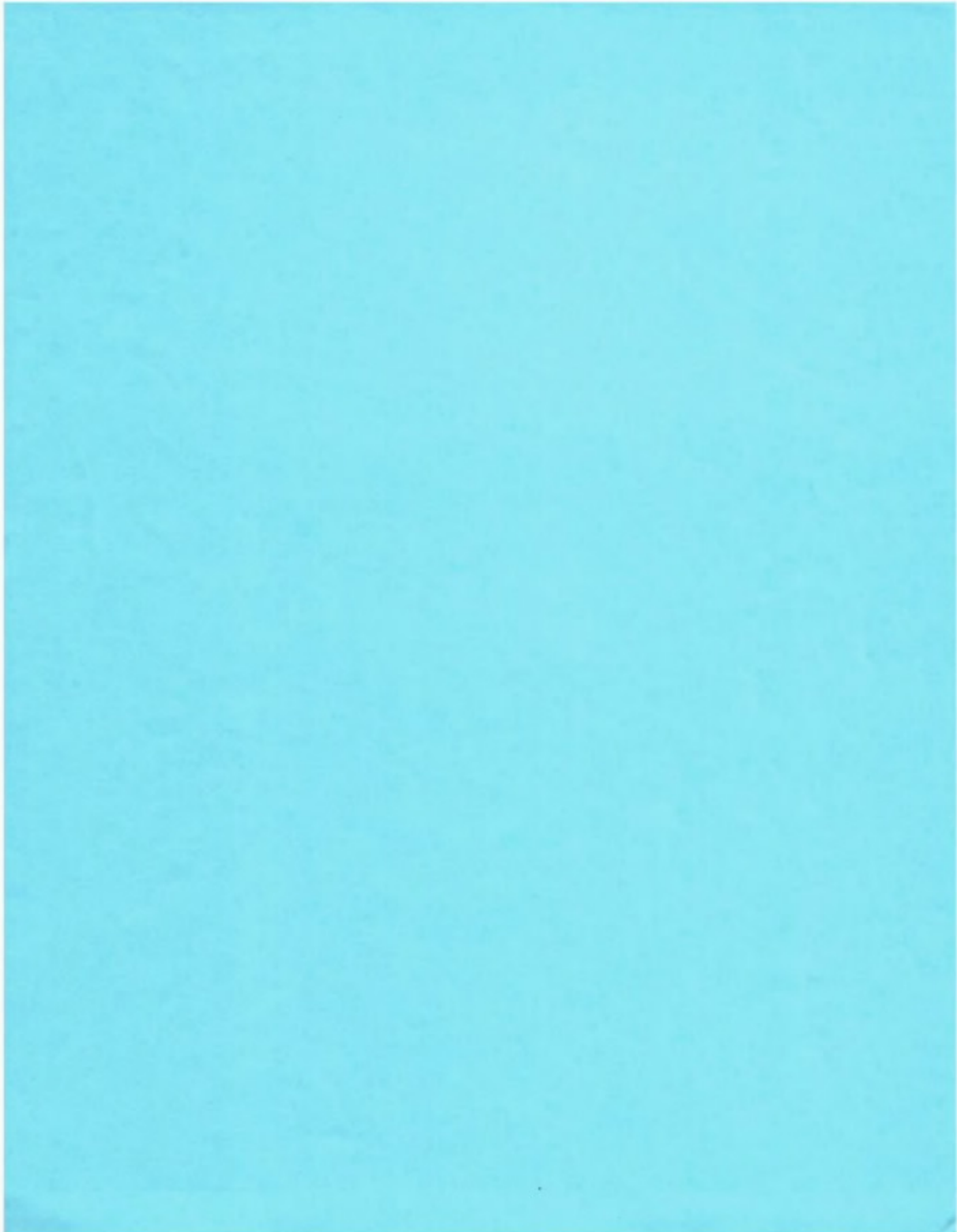
YOUR AGENCY'S USE OR DISCLOSURE OF THIS INFORMATION MUST BE IN ACCORDANCE WITH INTERNATIONAL HUMAN RIGHTS LAW, INCLUDING THE CONVENTION AGAINST TORTURE AND OTHER CRUEL, INHUMAN OR DEGRADING TREATMENT OR PUNISHMENT.

NO LETHAL ACTION MAY BE TAKEN ON THE BASIS OF THIS INFORMATION.

THIS INFORMATION IS FOR INTELLIGENCE PURPOSES ONLY AND MAY NOT BE USED IN LEGAL PROCEEDINGS. THIS INFORMATION MAY BE SHARED WITH MEMBERS OF YOUR GOVERNMENT WHO POSSESS THE REQUIRED SECURITY CLEARANCE AND A NEED TO KNOW. IT MAY NOT BE RECLASSIFIED, DISSEMINATED OR DISCLOSED, IN WHOLE OR IN PART, TO ANY OTHER GOVERNMENT OR ENTITY WITHOUT THE WRITTEN PERMISSION OF CSIS. IF YOU LEARN THAT THE DOCUMENT HAS BEEN IMPROPERLY DISCLOSED OR DISSEMINATED OR IF YOU ARE UNABLE TO ABIDE BY THE CAVEATS IN THIS DOCUMENT, INFORM CSIS IMMEDIATELY



For Public Release



For Public Release

Minister of Public Safety,  
Democratic Institutions  
and Intergovernmental Affairs



Ministre de la Sécurité publique,  
des Institutions démocratiques  
et des Affaires intergouvernementales

Ottawa, Canada K1A 0P8

DATE: SEP 19 2023

SECRET // CEO

The Honourable Marie Deschamps  
Chair  
National Security and Intelligence Review Agency  
99 Sparks Street  
Ottawa, Ontario

Dear Madame Deschamps:

Pursuant to subsection 6(2) of the *Canadian Security Intelligence Service Act*, my predecessor previously provided new direction to the Canadian Security Intelligence Service describing his expectations with regards to threats to the security of Canada directed at Parliament and parliamentarians.

Subsequent to that direction, Public Safety Canada and the Canadian Security Intelligence Service have developed a governance protocol to ensure an appropriate internal government process to support these disclosures. I have approved this protocol. I am providing this document to you so that the National Security and Intelligence Review Agency may have a complete record of general ministerial guidance provided to the Canadian Security Intelligence Service on this matter.

A handwritten signature in blue ink, appearing to read 'D. LeBlanc'.

The Honourable Dominic LeBlanc, P.C., K.C., M.P

Enclosure: (1)

Cc: David Vigneault, Director, Canadian Security Intelligence Service

The word 'Canada' in a bold, serif font, with a small Canadian flag icon above the 'a'.