

**CSIS and RCMP  
One Vision 2.0.**

**An Operational Approach to  
Intelligence and Evidence**

**CSIS - RCMP One Vision Strategic Meeting  
RCMP NHQ, January 26-27, 2016**



## Threat Management Framework

- Both CSIS and the RCMP share the goal of ensuring the safety and security of Canadians and protecting Canadian interests at home and abroad.
- This goal is most effectively accomplished through a sound and collaborative approach to threat management – the *One Vision* framework launched in 2012.
- *One Vision 2.0* enhances and codifies the existing framework for cooperation that guides deconfliction efforts and the disclosure of CSIS information to the RCMP.

# Intel to Evidence

- One Vision 2.0 is designed to formalize the transition of intelligence into the criminal justice system. It is recognized that the “intelligence to evidence” issue is complicated and evolving. It is subject to legislation and judicial precedent; it is informed by commissions of inquiry; it is affected by our respective policies and procedures; it is guided and assisted by training and mutual understanding.
- One Vision 2.0 creates a framework for cooperation that can be explained to and defended before the courts, and that maintains and creates both an appropriate degree of separation and a functionally operational relationship between CSIS and the RCMP.

*“It is my firm view that the distinction between policing and security intelligence should be restored, respected and preserved. I am convinced that Canadians will be best served if the RCMP and CSIS both operate within their distinct mandates and expertise, while sharing information when appropriate and working together in a cooperative and integrated manner”.*

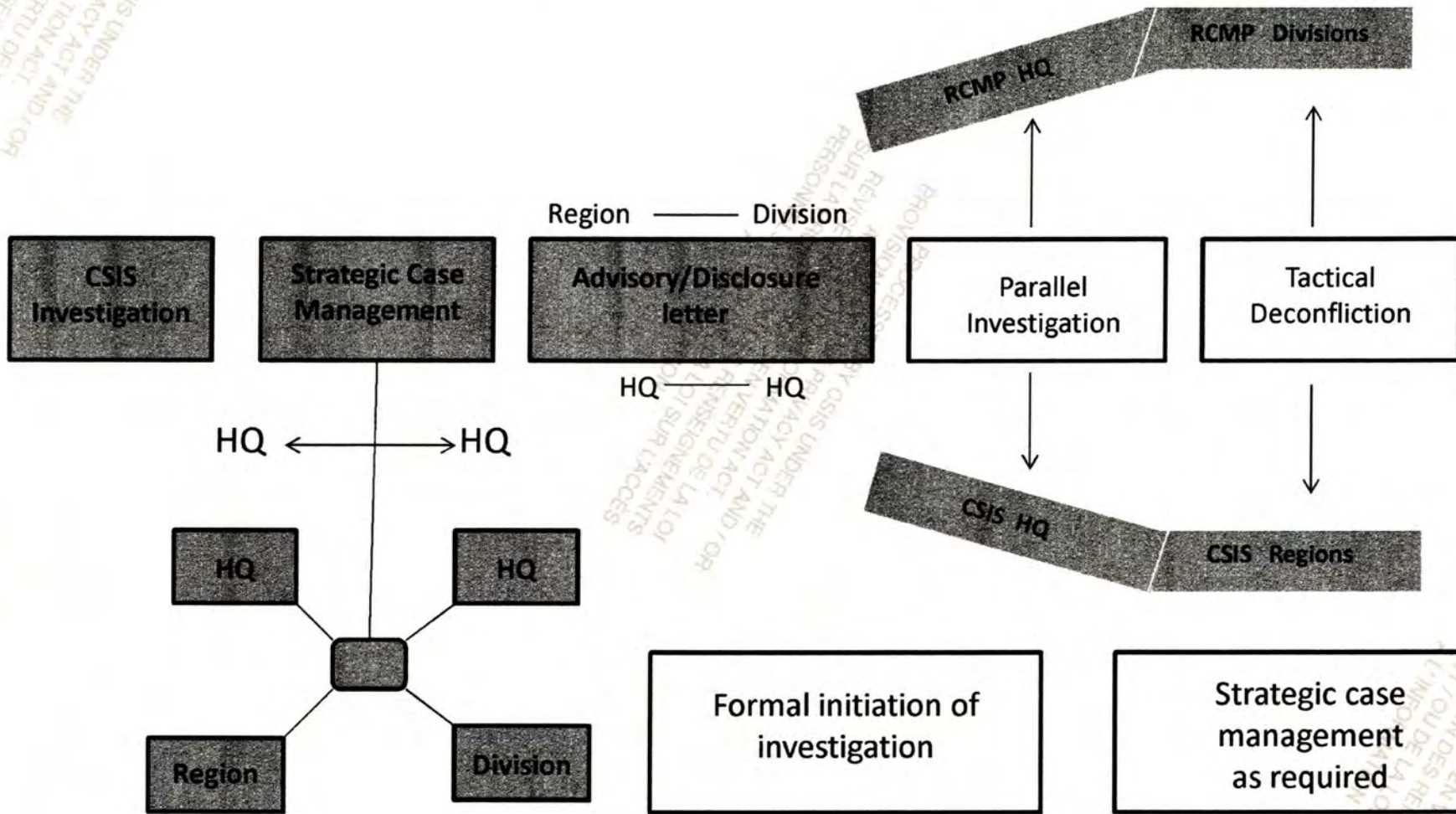
(Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar - hereinafter referred to as the “O’Connor Commission” - Report of the Events Relating to Maher Arar, Analysis and Recommendations, pg. 312)



# One Vision 2.0.

- Approved by the RCMP Commissioner and CSIS Director on 2015 11 24;
- Codifies – for the first time – the framework and the 5 principles;
- Provides key definitions to clarify the process and the roles of our respective HQs and Regions / Divisions;
- Serves as the Threat Reduction Activity (TRA) deconfliction mechanism;
- Formalizes and centralizes record keeping: RODs produced and approved by RCMP / CSIS HQ

# Intelligence and Evidence Flow



# Principles

- Public safety is paramount.

“Before I begin, however, I wish to draw attention to one pervasive feature of the RCMP’s national security role: the Force’s response to criminal threats to national security, like the government’s response to national security threats in general, is continuously evolving.”

(O’Connor Commission, ‘A New Review Mechanism for the RCMP’s National Security Activities, pg. 84)

*“To be sure, terrorism is a crime unto itself. It has no equal. It does not stop at, nor is it limited to, the senseless destruction of people and property. It is far more insidious in that it attacks our very way of life and seeks to destroy the fundamental values to which we ascribe - values which form the essence of our constitutional democracy.”*

(Court of Appeal for Ontario, R.v. Khawaja, Dec. 17, 2010, paragraph 231)

# Principles

- Always consider the effect of your actions upon the other agency.

“When information from a CSIS operation seeps into a police investigation it will often have to be disclosed. In some cases that can lead to the termination of prosecutions or police investigations in order to protect intelligence sources. That is highly undesirable from a police perspective. On the other hand, should intelligence gathering methods or sources used by CSIS be compromised by disclosure, for example during the criminal process, this can be very harmful to the effectiveness of CSIS operations on an ongoing basis. Consequently, both organizations have a distinct interest in maintaining a degree of separation between their operations. Avoiding such problems is clearly in the public interest.”

(Mr. Justice Dawson, Ruling No. 14, paragraph 33)

# Principles

- Earlier is better when discussing strategy, seeking legal advice, identifying problems and sharing information.

“At the risk of oversimplification, one of the main concerns is contaminating the police investigation with information gathered by CSIS pursuant to its separate mandate. When that occurs it creates problems for each organization in carrying out its respective role.”

(Mr. Justice Dawson, Ruling No. 14, paragraph 31)

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND / OR  
ACCESS TO INFORMATION ACT  
TRAITE PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION



# Principles

- Focusing the information to be disclosed by CSIS will assist both organizations and avoid future problems.

*“CSIS was giving limited information to the RCMP for the purpose of respecting the legislation under which it operates and to ensure that it maintained an appropriate degree of separation from the RCMP.”*

(Mr. Justice Dawson, Ruling No. 14, paragraph 65)

# Principles

- Every investigation is different; it is critical to have a consistent process which will recognize and manage these differences.

*“However, it is imperative that a special effort be made by all personnel in each institution to develop a better understanding and appreciation of the mandate and role of the other... Secondments and joint training and information programs would be ways of promoting better understanding and cooperation.”*

*(O’Connor Commission, Report of the Events Relating to Maher Arar, Analysis and Recommendations, pg. 319)*



# Foundational Criteria for National Security Criminal Investigations

- The initiation of a criminal investigation must be based on a reasonable suspicion or belief that criminal activity has occurred or may occur. The following may initiate a disclosure from CSIS to the RCMP:
  - Information and intelligence (foundational to the initiation of an investigation), which may indicate criminal activity ;
  - An element of an offence under the *Security Offences Act* or any other act of Parliament;
  - An imminent threat;
  - A pattern or behavior that may constitute a threat to the security of Canada.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND / OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION



# Assessment Process Prior to Disclosure Under Section 19, *CSIS Act*

- CSIS receives information and intelligence.
- CSIS makes an assessment which requires a consideration of:
  - The threat to the security of Canada;
  - The nature and seriousness of the potential criminal activity ;
  - The impact that sharing the information may have on the Service's investigations (sources, methods and operations, including the management of third party information);
  - The impact of judicial disclosure obligations on a CSIS investigation;
  - The merit and impact of involving other stakeholders (e.g. CBSA, CRA, foreign and domestic agencies).

PROCESSED BY CSIS UNDER THE  
ACCESS TO THE PRIVACY ACT AND / OR  
RÈGLEMENT PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

# Strategic Consultations

- If deemed appropriate by CSIS, CSIS HQ Ops Division will contact the RCMP to initiate a strategic case management meeting. (RCMP may initiate)
- The process will consist of a meeting(s) between the RCMP and CSIS to assess the magnitude and scale of the information and intelligence based on the foundational criteria.
- A decision will be made regarding the need for formal disclosure to the RCMP via Disclosure or Advisory Letter.
- A ROD will be produced by CSIS, agreed to by both organizations and retained on our respective files.
- TRA will be deconflicted if applicable (RCMP engagement on a file may result in TRA being held in abeyance).



# Assessment Process Prior to Disclosure Under Section 19, *CSIS Act*

- It is recognized that, depending on the nature of the case, the RCMP will wish to be informed about the following information:
  - The subject of the investigation (“who”);
  - The activity (“what”);
  - The time frame (“when”);
  - The location (“where”);
  - The motivation, if known (“why”)
- The content of disclosures will be discussed at the strategic case management meeting.

# Disclosure Under Section 19, *CSIS Act*

- Contingent upon the results of the strategic case management meeting, CSIS may initiate a disclosure process.
- The RCMP will, upon receipt of the letter, disseminate as deemed appropriate (SOPs and guidelines being developed).
- As soon as practical, the RCMP will advise CSIS of what investigational avenue the RCMP will pursue, if any, based on the information and intelligence CSIS shared.

# During the Criminal Investigation

- Adherence to these guidelines will help ensure that the RCMP criminal investigation remains separate, distinct and parallel to any CSIS investigation.
- It is recognized that there will be a continuing need for coordination and de-confliction between the two investigations that may lead to disclosure.

“... they understood the need to share certain information of fundamental importance while ensuring a careful separation between their investigations. The evidence indicated that care was taken to ensure that there was a form of “firewall” between the two organizations, through which only certain limited information would be permitted to pass. ...Mr. Brooks and Inspector Jagoe understood that certain information would only be used by Inspector Jagoe for strategic purposes, such as the allocation of resources.”

(Mr. Justice Dawson, Ruling No. 14, paragraph 41)



# During the Criminal Investigation

- There is a continuing requirement for CSIS to report to government on threat-related activities and the RCMP can assist in that regard.
- Primacy does not mean exclusivity.

“The evidence reveals that there was a much larger flow of information from the RCMP to CSIS than the other way around ...CSIS came to rely on the RCMP providing information from the Osage investigation to satisfy aspects of CSIS's mandate. The evidence is quite clear, however, that the information flow from CSIS to the RCMP was very limited and carefully controlled.”

(Mr. Justice Dawson, Ruling No. 14, paragraph 43)

# During the Criminal Investigation

- Ongoing inter-agency dialogue may be appropriate to ensure public safety concerns are met and all options are explored.
- These will take the form of strategic case management meetings or, as required, tactical deconfliction.

“The evidence established that the JMT’s involved other agencies and police forces as well, and I am satisfied that the exchange of information was restricted to ensuring awareness of each other’s general operations and projects for management purposes. .. The evidence did not reveal that such meetings were used to pass detailed information that might be regarded as fruits of the investigations.”

(Mr. Justice Dawson, Ruling No. 14, paragraph 40)

# During the Criminal Investigation

- CSIS, when conducting a parallel investigation, may disclose additional information and/or intelligence consistent with the One Vision principles. (Important to maintain the separation of investigations)
- The RCMP will provide CSIS with information and/or intelligence. (No jeopardy and allows for more effective deconfliction).

“While CSIS faces potentially adverse consequences as a result of sharing information with the police, there are no similar consequences for other agencies that share information with CSIS. There is no excuse for any agency failing to share information with CSIS. Security-related threat information collected by the RCMP for law enforcement purposes can, and ought to be, shared with CSIS in all but the rarest of circumstances. The Commission does not view the report or recommendations of the O’Connor Commission as being in any way inconsistent with this observation.”

(Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 - hereinafter referred to as the “Air India Commission” - Volume One, *The Overview*, pg. 167)

- In accordance with policy, CSIS and the RCMP will ensure the retention of information, intelligence and evidence.



# Post Investigation / Pre-trial Disclosure (Stinchcombe)

- The responsibility for disclosure belongs to the Crown.
- Ongoing inter-agency (including DOJ and PPSC) strategic consultation to ensure the appropriate use of sensitive national security information and its protection as required.
- CSIS investigations are separate and distinct from RCMP criminal investigations. CSIS is normally a third party for disclosure purposes.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND / OR  
ACCESS TO INFORMATION ACT.  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

# • Questions?

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND / OR  
ACCESS TO INFORMATION ACT.  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND / OR  
ACCESS TO INFORMATION ACT.  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION