UNCLASSIFIED

2021/11/10

CSIS–RCMP Framework for Cooperation

One Vision 3.0

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

UNCLASSIFIED

TABLE OF CONTENTS

UNCLASSIFIED

BACKGROUND

Both the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) share the goal of ensuring the safety and security of Canadians and protecting Canadian interests at home and abroad. This is most effectively accomplished through a sound and collaborative approach to threat management.

Cooperation at the earliest possible stage allows for a collaborative assessment of the threat, including whether threat reduction activities may be appropriate in the circumstances. This consultation also provides the opportunity to determine which party may be best placed to act on a specific threat on a case-by-case basis. However, this collaborative approach neither replaces nor impedes either agency's prerogative to make independent operational decisions consistent with their respective mandates and applicable laws.

The *One Vision* initiative, launched in 2012, reflected a culmination of efforts to enhance the RCMP and CSIS relationship given the challenges inherent in the utilization of intelligence as evidence in prosecutions. To date, *One Vision* has been an effective framework, underlining the importance of continued collaboration and information sharing in support of the RCMP's and CSIS' mandates. It has also served to maintain the necessary independence between respective investigations while ensuring a functional, operational relationship. Its development was informed by recommendations stemming from commissions of inquiry, supported by decisions of the courts and strengthened by case management experience.

Since *One Vision* was launched, there have been significant changes in Canada's national security landscape (i.e. the threat environment and legislative amendments to the *Criminal Code of Canada* and the *CSIS Act*), which have changed the way that CSIS and the RCMP cooperate in the national security space. For instance, CSIS' mandate to reduce threats through the use of Threat Reduction Measures (TRMs) introduced a need for specific deconfliction to ensure TRM measures do not adversely affect RCMP activities. Given these changes, a new framework was formalized in 2015, entitled *One Vision 2.0*.

In 2018, CSIS and the RCMP proactively initiated a review by an independent third party to assist in identifying challenges and solutions to improve cooperation. The *Operational Improvement Review* (OIR) resulted in 76 recommendations aimed at improving operations, updating policy, modernizing training and suggesting legislative reform. In addition, the OIR identified new opportunities for the involvement of the Public Prosecution Service of Canada (PPSC) within the national security (NS) space. Implementation of the OIR recommendations coupled with the new PPSC roles necessitated an updated framework, *One Vision 3.0*.

As identified in the OIR, CSIS and the RCMP need to adapt their culture to accept that prosecution is no longer considered to be the 'gold standard' of threat mitigation, as there are many threats for which a criminal prosecution is neither appropriate nor the most effective threat management measure. The evolution of the *One Vision 3.0* framework demonstrates CSIS' and RCMP's commitment to improvements as new challenges arise, to learn from experiences, and embrace new strategies to continue to ensure public safety in Canada and internationally.

UNCLASSIFIED

KEY TERMS & DEFINITIONS

Information Sharing
Information sharing refers to the provision of information from the RCMP to CSIS, or from CSIS to the RCMP, in accordance with the *One Vision* framework. Information sharing is vital to both CSIS and RCMP operations and to the fulfillment of their respective mandates. For CSIS, this term is synonymous with disclosure, pursuant to s. 19 of the *CSIS Act*.

Disclosure
In the context of an RCMP investigation or a criminal prosecution, disclosure refers to the production of records and information to a court, person or body with jurisdiction. For CSIS, disclosure is more broadly defined and understood to be the provision of information to persons or organizations outside CSIS, pursuant to s. 19 of the *CSIS Act (see below).* For the purposes of this document, "disclosure" has the meaning used in the context of RCMP investigations or criminal prosecutions.

CSIS Information Sharing Authority
CSIS primarily derives its authority to share information with the RCMP from s. 19 (2)(a) *CSIS Act*, *"where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or province, to a peace officer having jurisdiction to investigate the alleged contravention."*

RCMP Information Sharing Authority
The RCMP primarily derives its authority to share information with CSIS from s. 18 of the *RCMP Act* under the duties assigned to peace officers to preserve the peace, prevent crime and offences against the laws of Canada. In addition to the *RCMP Act*, the RCMP derives authority to share information with CSIS from s. 6(1) of the *Security Offences Act* which provides the RCMP with the primary responsibility of performing the duties assigned to peace officers in relation to offences that constitute a threat to the security of Canada within the meaning of the *CSIS Act* and offences against internationally protected persons as defined by s. 2 of the *Criminal Code.*

Strategic Case Management Meeting (SCM)
A consultative process whereby the RCMP and CSIS, either with or without PPSC, will meet to discuss the nature of the threat(s) and determine the best approach moving forward in line with their respective mandates and authorities. These meetings are also used to discuss the possible use of Threat Reduction Measures by CSIS and any potential impact on the RCMP's ongoing and future activities. These meetings can be in the form of a 2, 3, 4 or 5 Pillar SCM meeting.

Tactical Deconfliction (TD)
A meeting between CSIS regional and RCMP divisional management level representatives designed to resolve or eliminate operational activities that interfere with the other party's investigation. TD meetings must not be used to discuss any Threat Reduction Measure. Except in cases of imminent threat (i.e., threat to life or threat of serious bodily harm), these meetings will not include any information sharing on the part of CSIS. Should CSIS verbally share information in the case of an imminent threat, a Use Letter prepared by CSIS Headquarters (HQ) will follow.

UNCLASSIFIED

Use Letters
A Use Letter describes the information that CSIS wishes to share with the RCMP and contains caveats expressly outlining the use of the information[1].

CSIS Threat Reduction Measures (TRM)
A CSIS operational measure undertaken pursuant to s. 12.1 of the *CSIS Act* for which the principal purpose is to reduce a threat as defined in s. 2 of the *CSIS Act.*

Headquarters (HQ) Level
This term refers to the employees, and the activities of, the RCMP and CSIS at their respective Headquarters in Ottawa. Headquarters personnel are responsible for providing necessary guidance and strategic case management to activities undertaken at the regional/divisional level.

Divisional/Regional Level
This term refers to the employees of, and the activities of, the RCMP at the divisional level and Liaison Officers deployed abroad, and CSIS at the regional level. Divisional/regional personnel are responsible for the day-to-day operations and investigative activities.

Record of Decision (RoD)
A Record of Decision (RoD) documents any decision taken during either a Strategic Case Management meeting or a Tactical Deconfliction meeting and the supporting rationale. While RoDs are written only by CSIS, RoD handling protocols are specific to each organization and both organizations retain an identical copy.

[1] CSIS now refers to all information sharing letters as "Use Letters" containing dedicated caveats. This terminology replaces the previous process of sharing information through "Disclosure Letters" or "Advisory Letters".

UNCLASSIFIED

MANDATES

The RCMP is Canada's national police force with a broad mandate derived from common law, legislation and legal precedent. The RCMP is mandated to prevent and investigate crime in Canada and extraterritorially; maintain peace and order; enforce laws; contribute to national security; ensure the safety of state officials, visiting dignitaries and foreign missions; and provide vital operational support services to other police and law enforcement agencies within Canada and abroad. As such, the RCMP has the primary responsibility to perform the duties assigned to peace officers in relation to national security investigations and offences in the *Security of Information Act* and the *Security Offences Act.*

CSIS' mandate is to investigate, within Canada and abroad, activities suspected of constituting threats to the security of Canada by collecting, analyzing and retaining information and intelligence with respect to those activities and report on these to the Government of Canada. CSIS may also undertake measures, within Canada or abroad, to reduce threats to the security of Canada in accordance with well-defined legal requirements and Ministerial Direction. In short, if there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, CSIS may take measures to reduce the threat.

ONE VISION: PURPOSE

The purpose of the One Vision framework is to establish a clear and transparent framework to govern information sharing between CSIS and the RCMP as they both exercise their separate national security mandates. One Vision is the foundation that supports the overall operational relationship between CSIS and the RCMP and allows each agency to maintain an appropriate degree of independence.

OVERARCHING PRINCIPLES

Five principles underpin the CSIS-RCMP *One Vision* Framework:

1. ***Public safety is paramount – it is the true Gold Standard***

Addressing national security threats to Canada and Canadians to ensure public safety is the number one priority for both the RCMP and CSIS. Both acknowledge that while investigations must be independent, CSIS and the RCMP must carry out their respective mandates in a parallel yet collaborative fashion to ensure public safety. Both agencies must think critically about which approach may be most effective to manage the threat, including by leveraging all available tools, and those of partners.

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

Parties recognize that issues must be addressed at the earliest possible stage to maximize the number of available options, including those other than criminal prosecution. Adherence to this

practice and associated documentation of decision-making will demonstrate transparency and accountability in regards to each parties' activities to the government, the public and the courts.

3. ***CSIS' careful assessment of its intelligence prior to sharing it with the RCMP will assist both organizations and reduce disclosure challenges***

To continue to detect and disrupt threats to Canadians at home and abroad, CSIS and the RCMP must maintain robust dialogue, continued engagement, and enhance information sharing. CSIS will conduct a comprehensive assessment of the impact of information sharing while protecting its sources and methods, with input from the RCMP and PPSC as necessary. RCMP will then evaluate whether any CSIS information shared is useful to the RCMP in pursuing its law enforcement mandate. At all times, information sharing by both CSIS and RCMP will be conducted in a manner consistent with their respective mandates, keeping in mind the preservation of CSIS' status as a third party to any criminal investigation and also the PPSC's disclosure obligations.

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

The parties recognize that because every investigation is different, periodic consultations may be required for each case to account for the specific context and circumstances. As such, a consistent outlined process for cooperation is necessary while remaining sufficiently flexible to manage cases and maintain the ability to respond to evolving threats.

5. ***Personnel should consider the effect of their actions upon the other agency while maintaining autonomy in their decision-making***

As the RCMP and CSIS conduct separate parallel investigative activities, there is a potential that either agency may inadvertently negatively affect the other's current or future investigations, or potential criminal prosecutions due to protections afforded to human or technical sources, collection methodology, etc. Both parties agree that they should continue to be mindful of not only their own mandate, but also that of the partner agency. At the same time, the parties shall ensure that decision-making occurs separately, guided by each agency's own distinct mandate and internal approval mechanisms.

ONE VISION 3.0: INFORMATION SHARING PROCESS

Information sharing[2] from CSIS to the RCMP can take the form of a "Use Letter" or a meeting, namely Strategic Case Management (SCM) or Tactical Deconfliction (TD), as discussed under forums for cooperation/information sharing below. In order for CSIS to determine if and in what form it will share information with the RCMP, it must consider a number of factors. These include the public interest in sharing information, the impact that sharing may have on CSIS' investigations and equities (sources, methods and operations, including third party information), as well as the impact of any judicial disclosure obligations on CSIS. The RCMP will then need to

[2] As noted in the key terms section, for CSIS, information sharing to the RCMP is referred to as "disclosure" as that term is used in s. 19 of the *CSIS Act*.

determine whether the CSIS information, taking into account any limitations on the use of the information, will assist the RCMP in fulfilling its mandate. CSIS and the RCMP, with the assistance of PPSC counsel as appropriate, may discuss their respective understandings of the foregoing matters, as well as mitigation strategies that can maximize the ability to address the public interest in sharing, while minimizing potential adverse impacts on CSIS' ability to fulfill its mandate. This includes addressing the need to safeguard sensitive or potentially injurious information in the course of a prosecution and the potential impact of such measures on a prosecution.

Methods of Information Sharing

CSIS' sharing of its information may take the form of Use Letters, which state the purpose for which the information can be used, or verbally during One Vision 3.0 meetings (SCM or TD). Information shared by CSIS verbally in a SCM or TD is caveated: its use is restricted to inform the discussion at a SCM or TD meeting and it must not inform any law enforcement investigative action or step unless it is separately provided in a subsequent Use Letter. A Use Letter will be clearly caveated to identify to whom and how the RCMP may disseminate the information and as agreed to during the SCM meeting. The exception to this is in cases of imminent threat (i.e. threat to life or threat of serious bodily harm) wherein a verbal disclosure may be acted upon and a properly caveated Use Letter will follow from CSIS HQ to RCMP HQ.

If a Use Letter is provided containing information that may be used by the RCMP to obtain judicial authorizations, CSIS requires the opportunity to review applications prior to filing. As above, the information in the Use Letter is not to be used as grounds in support of a judicial application by the RCMP without prior approval from CSIS.

Ongoing Information sharing requirements

CSIS does not gather information as part of a criminal investigation, and its materials are not fruits of the investigation and therefore are not subject to *Stinchcombe* disclosure obligations. CSIS, with the support of legal advice from Justice Canada's National Security Litigation and Advisory Group (NSLAG aka Departmental Legal Services (DLS)), must assess what should be disclosed to the RCMP when it is in possession of information that has been identified as being obviously relevant. This includes information that:

- Tends to raise a doubt as to the accused's factual guilt, including information that directly undermines the credibility of a material witness in relation to the commission by the accused of the offence;
- Tends to show unlawful acts which could result in a finding of inadmissibility or abuse of process in the criminal proceeding;
- Relates to a Threat Reduction Measure in relation to the accused.

In an effort to achieve the above, the RCMP will share with CSIS, in a timely manner, relevant operational information, including information on its national security investigations and efforts to mitigate the threat through other actions within its mandate.

The parties agree that they will update each other concerning substantive changes related to previously shared information, including corrections, during SCM meetings. This will ensure that any subsequent activities taken by either organization are properly informed. Updates should also be given when there are changes in threat mitigation strategies such as:

- Likelihood of proceeding with arrest and criminal charges;
- Use of alternate federal statutes or non-terrorism offences to mitigate risk (e.g. consideration of drug, fraud, assault charges, immigration, etc.);
- Peace bond applications (terrorism related or traditional – e.g. a Court order that imposes conditions to prevent offences, including instituting a curfew, wearing of ankle/monitoring system, weapons prohibition, restraining order, etc.).

It remains imperative that CSIS has visibility over the investigative yield from the RCMP that would allow CSIS to stay informed about a particular national security threat and thereby adjust its intelligence investigation.

Forums for Cooperation/Information Sharing

- Strategic Case Management meetings[3]:
  - 2 Pillar (CSIS HQ / RCMP HQ or CSIS HQ/PPSC)
  - 3 Pillar (CSIS HQ/RCMP HQ/PPSC)
  - 4 Pillar (CSIS HQ/RCMP HQ/ CSIS regions and RCMP divisions)
  - 5 Pillar (CSIS HQ /RCMP HQ/regions/divisions/PPSC)

- Tactical Deconfliction meetings (CSIS regions/RCMP divisions) (Open/Closed).

Strategic Case Management Meetings (2 or 3 Pillar)

A 2 or 3 Pillar SCM meeting will be held at Headquarters (CSIS or RCMP) and include management level participants or delegates who possess the necessary decision-making authority. Divisional/regional representatives do not participate in 2 or 3 Pillar meetings but should be aware of their occurrence and privy to the decisions made. The purpose of these meetings is to discuss and assess the nature of the threat and collaboratively determine the most effective way to manage it. Information shared by CSIS verbally in a SCM is caveated: its use is restricted to inform the discussion at the SCM and must not inform any law enforcement investigative step or action, unless separately provided in a subsequent Use Letter. These meetings may be convened by either party. The party that convenes the meeting is responsible for chairing the meeting, and maintaining the meeting's direction and focus.

If both parties require guidance from PPSC on a specific issue, PPSC can be invited to the meeting – known as a 3 Pillar. PPSC's participation is governed by the 2020 *Memorandum of Understanding between the Department of Justice (DOJ), PPSC, RCMP and CSIS concerning certain roles and responsibilities in relation to national security investigations*. Both parties

[3] Note that CSIS HQ can also include National Security Litigation Advisory Group (NSLAG/DLS) participation for the purpose of providing legal advice to CSIS.

must clearly identify the area of advice sought from PPSC to focus and streamline the discussion. After PPSC has provided its advice in the meeting (or following such a meeting), a regular 2 Pillar meeting will be convened to decide on a way forward to ensure operational independence of both agencies.

Strategic Case Management Meetings (4 or 5 Pillar)

A 4 Pillar SCM meeting may be convened by either party to discuss the threat or investigation and to solicit additional context from the regions/divisions. When engaged in parallel investigations, it is strongly recommended that 4 Pillar SCM meetings occur as often as required to ensure each agency is making decisions based on the most current facts available.

This meeting serves to ensure a common understanding of the nature of the threat and each agency's intended response. Early and ongoing SCM meetings will ensure each agency is able to continue its parallel investigation with minimal impact on the other. These discussions can take place either in person or via secure video teleconference and, to the extent possible, be hosted equally between CSIS and RCMP facilities. A Use Letter may follow with the appropriate caveats. Either party may convene these meetings. The party that convenes the meeting is responsible for chairing the meeting and maintaining the meeting's direction and focus.

If both parties require guidance from PPSC on a specific issue, PPSC can be invited to the meeting – known as a 5 Pillar. Both parties must clearly identify the area of advice sought from PPSC to focus and streamline the discussion. After PPSC has provided its advice in the meeting (or following such a meeting), a regular 4 Pillar meeting will be convened to decide on a way forward to ensure operational independence of both agencies.

The SCM meeting (usually a 2P or 4P) is the venue CSIS will use to discuss its Threat Reduction Measures (TRM). Note that prior to CSIS undertaking a TRM, CSIS must first consult, where appropriate, with other federal departments or agencies as to whether they are in a position to reduce the threat; CSIS must consult with the RCMP on all TRM's related to s. 2(c) of the *CSIS Act.* Consultations are managed via *One Vision* as referenced in CSIS TRM policy.

Further to these discussions, the RCMP will advise CSIS that it either has no objections to the TRM or request additional time to review and assess for potential conflict with a RCMP investigation. The RCMP will provide its response in a timely manner. Should the RCMP open a future file on the subject of a CSIS TRM, the RCMP will initiate a follow-up SCM meeting to discuss what, if any, TRM was employed. This will facilitate the RCMP's assessment of any implications for the criminal investigation.

Tactical Deconfliction Meetings (Open and Closed)

The purpose of TD is to resolve or eliminate operational activities that interfere with the other party's investigation. As such, information shared during a TD meeting is different from that shared during a SCM meeting. TD could include:

- Notification when planning the deployment of surveillance teams to avoid covering the same subject of investigation (SOI) at the same time;
- Notification when planning to conduct an interview of a subject in case both agencies plan to speak to the same person;
- Consultation about undercover operations.

There are two types of TD meetings, which delineate the level of RCMP personnel in attendance: Open and Closed. Open allows the RCMP investigative team to be present and aware of the topics being discussed, while Closed precludes the attendance of the RCMP investigative team to maintain a sterile corridor that serves to enhance the protection of sources, tactics, sensitive intelligence and the integrity of the police investigation. TD meetings must not be used to make decisions regarding CSIS Threat Reduction Measures. In addition, any information shared by CSIS verbally in a TD meeting is caveated: its use is restricted to inform the discussion at the meeting and it must not inform any law enforcement investigative step or action, unless it is separately provided in subsequent Use Letter. The exception to this is in cases of imminent threat (i.e. threat to life or threat of serious bodily harm) wherein a verbal disclosure can be made and a properly caveated Use Letter will follow from CSIS HQ to RCMP HQ.

Either party may convene these meetings. The party that convenes the meeting is responsible for chairing the meeting and maintaining the meeting's direction and focus.

ROLE OF THE PUBLIC PROSECUTION SERVICE OF CANADA

PPSC has primary responsibility for providing legal advice in relation to a prospective prosecution as defined in the *Director of Public Prosecutions Act*. PPSC may also provide legal advice to CSIS where the advice would be relevant to a law enforcement investigation or criminal prosecution. All advice provided by the PPSC to the RCMP, CSIS, NSLAG or other Government of Canada department or a province, is in respect to the actual or potential exercise of prosecution discretion as defined in the *Director of Public Prosecutions Act*.

In accordance with relevant Memorandums of Understanding, this Framework establishes that PPSC may provide advice to both CSIS and the RCMP during SCM meetings.

The PPSC may also meet and provide advice directly to CSIS apart from the RCMP. PPSC advice to CSIS may include the following:

- Advice that is general in nature about aspects of criminal law that may become relevant where the CSIS information surfaces or is used in a law enforcement investigation or criminal prosecution;
- Advice as to whether or not information and intelligence obtained by CSIS in the course of an investigation carried out under s. 12 of the *CSIS Act* which relates to a specific individual or entity, or obtained incidentally in the course of its duties and functions, is indicative of criminal activities such as could be investigated by the RCMP. The advice is provided in a context intended to assist or serve CSIS in making a decision on disclosure under s. 19 of the *CSIS Act*.

PPSC may also provide advice to CSIS with NSLAG on questions related to whether the disclosure of the identity of a human source is essential to establish an accused's innocence for the purposes of s. 18.1(4) of the *CSIS Act*.

RECORD OF DECISION

Strategic Case Management (SCM) Meetings
CSIS HQ is responsible for writing the Record of Decision (RoD) and disseminating it to attendees including the RCMP.

Content

This record will reflect any decisions taken as well as the underlying rationale. The RoD will follow a mutually agreed template and include the following elements, as applicable:

- Attendees;
- Sufficient information about the threat, including basic identifying details (e.g. name and date of birth), to determine collectively the best approach to address it;
- Where the RCMP has indicated a potential or actual conflict with RCMP operations, a brief explanation of the reason(s), as applicable;
- Reference past CSIS Use Letters;
- Action items (e.g. Use Letter to follow) ;
- Sufficient information about the Threat Reduction Measure to enable the RCMP to assess whether the proposed measures would interfere with RCMP activities.

Tactical Deconfliction (TD) Meetings

CSIS regional personnel are responsible for writing the RoD and disseminating it to their RCMP divisional counterparts for all TD meetings. TD RoD templates are to be detailed enough to provide an accurate reflection of the discussion and provide an account of decisions made, the supporting rationale, and the required follow-on action by each party, as relevant. It need not include the same level of detail that would normally be found in meeting minutes.

Recordkeeping

All SCM RoDs will be documented to file at CSIS HQ and RCMP HQ. The RoD will be circulated to both CSIS and RCMP attendees, including at the regional and divisional levels. Information handling protocols will be developed at the regional/divisional level to ensure the RoDs are kept in compliance with CSIS and RCMP policies. If PPSC participated in the meeting, they may view the RoD at either CSIS or RCMP offices, dependent upon protocols to be developed within each region/division.

CSIS regional personnel will write RoDs for all TD meetings using the TD RoD template and disseminate it to the appropriate RCMP divisional personnel in accordance with CSIS procedure and guidelines. Information handling protocols will be developed at the regional/divisional level to ensure the TD RoDs are kept in compliance with CSIS and RCMP policies.

UNCLASSIFIED

AGREEMENT

****

The terms herein have been agreed by both parties.

Director,	**Commissioner,**
Canadian Security Intelligence Service	**Royal Canadian Mounted Police**
Date: 2021/11/29	**Date:** 2021·11·29