Protected B

Intelligence and Evidence: Challenges and Possible Legislative Reforms

Pre-brief for ADM Roundtable with Experts

NS-Strat Pol & IE2 Team

April 4, 2022

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Presentation Overview

Protected B

- The Intel to Evidence Challenge
  - History, Efforts to Date, and WhyNow?
- Potential Reforms: Proposals from the Experts
  - Additional legislative reforms under consideration by the Government of Canada
- Discussion Questions for the Roundtable

Tomorrow's Meeting

Protected B

- Following the NS Info-Sharing Symposium on March 21st, the PS and CSIS ADMs sought to organize a closed-door follow-up roundtable with the expert panellists to discuss legislative reform.

- Experts are: **Anil Kapoor** (Criminal Defence and Regulatory Lawyer, Kapoor Barristers), **Leah West** (Assistant Professor, Carleton University), **Solomon Friedman** (Criminal Lawyer, Friedman Mansour LLP), **Croft Michaelson** (VP & Chief Legal Officer, BMO Financial Group; former Crown Prosecutor)

- During the Symposium, experts presented long-standing and new legislative reform options.

- Tomorrow's meeting is intended to offer ADMs the opportunity to learn more about the new proposed solutions.

Canada

Canada

Department of Justice Canada

Public Prosecution Service of Canada

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

The I&E Challenge

Protected B

The I&E challenge refers to the operational and legal challenges encountered when sensitive information is used to inform criminal investigations and legal proceedings, or other government action to address national security threats (including threat disruption/mitigation).

The challenge arises from (1) the need to protect how information is obtained and assessed for national security purposes, and (2) the legal obligation to disclose relevant information to a person accused of a crime or otherwise subject to legal proceedings.

It is one of the greatest challenges to NS investigations in Canada

The I&E Challenge in Practice

Protected B

- The RCMP frequently relies on third party, sensitive information to begin or advance NS investigations.

- Should this information be relevant to the charges or an issue at trial, it will have to be disclosed during a judicial process

- Risk: information will need to be privileged and thus may not be useable in court. Defense can also request further disclosure from third parties (e.g. CSIS), leading to greater disclosure obligation risk and time used (risk to *Jordan* timeline)

- Failure to manage sensitive information can lead to remedies adverse to the Crown (e.g. dismissing charges, staying proceedings), a failure to uphold public safety, and an enormous waste of law enforcement resources

I&E History

Protected B

- 2008: Review of Large and Complex Criminal Trials in Canada (Lesage & Code)
- 2010: Air India Inquiry
- 2012: CSIS-RCMP One Vision Framework
- 2015: CSIS-RCMP One Vision 2.0
- 2017: Operational Improvement Review & United Kingdom Deployment
- 2019: NSIRA Annual Report
- 2020: NSIRA Report on CSIS-RCMP Relationship
- 2021: Mandate Letter Commitment

"Expand[…] collaboration and information and intelligence sharing with Canadian partners and all orders of government […]" & "[…] strengthen the capacity of Canadian police and prosecutors to bring to justice […] terror suspects to the fullest extent of the law."

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

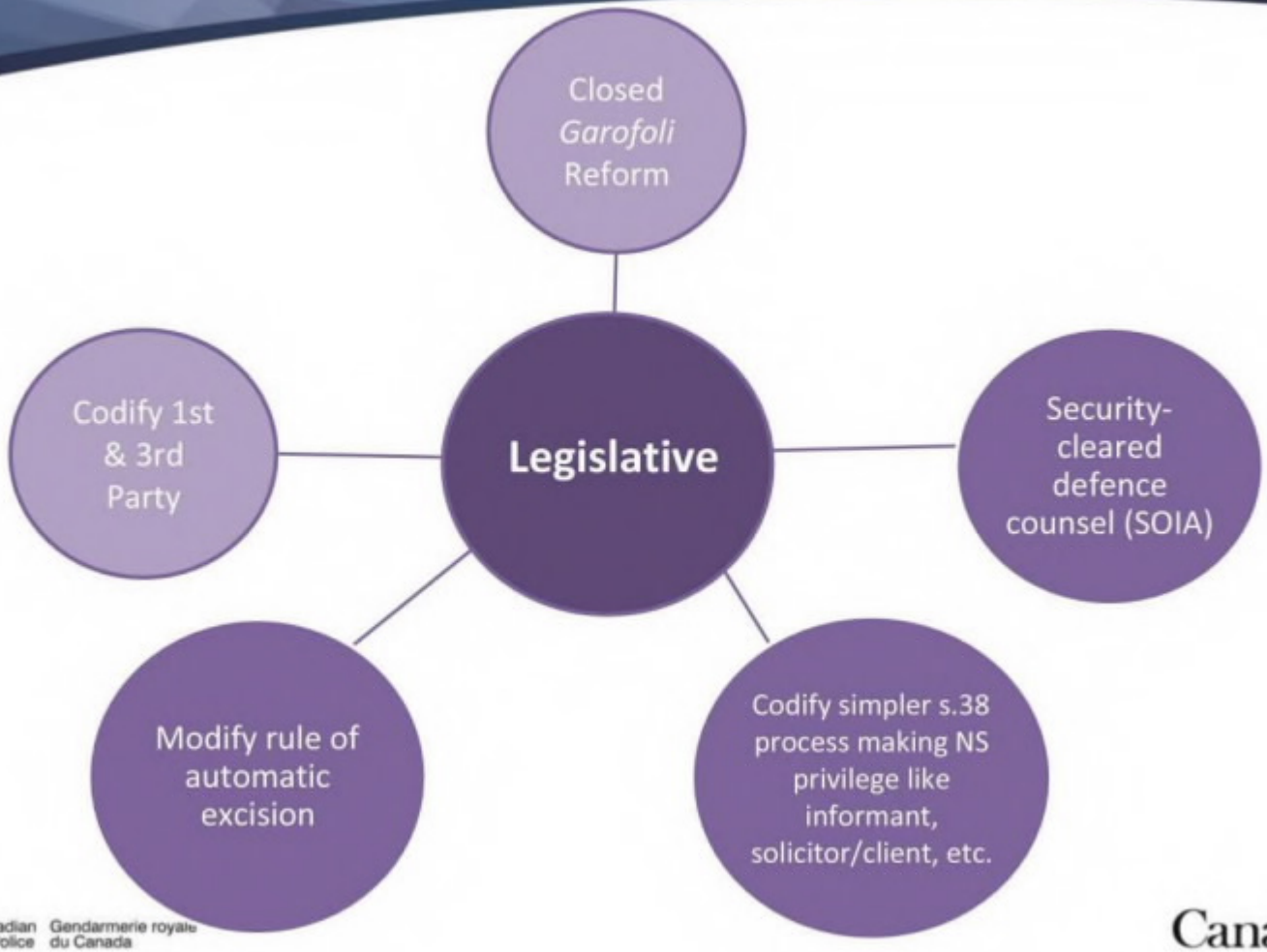
Recent Operational Progress

Protected B

- The RCMP has made significant operational progress in the last 3-4 years:
  - Majority of OIR & UKD **Recommendations have been Resolved or Actioned**
  - **A Joint-MOU** governing information sharing was signed in October 2020 by the RCMP, CSIS, the PPSC, and DOJ
  - The **One Vision 3.0 Framework**, which governs operational collaboration between FPNS and CSIS was signed by the Commissioner and Director in November 2021
  - CSIS Use Letter Guidance and Handling Instructions forthcoming this spring
  - Secure Communications infrastructure between CSIS and the RCMP has been upgraded

Key Issues for Tomorrow

Protected B



Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Other Known Legislative Issues

Protected B

In addition to the reforms raised by the experts, there are other known legislative options that may be raised by GoC participants to gauge the experts' sense of how beneficial these reforms could be to addressing the I&E dilemma:

- **Closed Material Proceedings (CMPs): SARP, *Garofoli*, terrorism peace bonds**
- **Barring Interlocutory Appeals**
- **Repealing Bifurcation**
- **Codifying 1st and 3rd Party Regimes (*Stinchcombe* and *O'Connor* reform)**
- **Sealing Warrants on NS Grounds**

Closed Material Proceedings

Protected B

- CMP: proceedings are conducted in camera (i.e. closed to public) and *ex parte,* meaning that the defense is not present. A CMP allows the judge to rely upon the withheld information, whereas section 38 does not.

- CMP can enhance security but risks violating the *Charter* rights of the defense to a fair and open trial. A CMP regime **does not exist** in the criminal context .
  - Remedies include having an *amicus curiae* present to argue on behalf of defense, issuing summaries of material / proceedings, etc. (the authority to appoint an *amici* would first need to be enshrined in legislation)
  - CMP is used variously in our judicial system, for instance in judicial reviews of *Immigration and Refugee Protection Act* Security Certificate cases or the imposition of publication bans or exclusion of the public

-

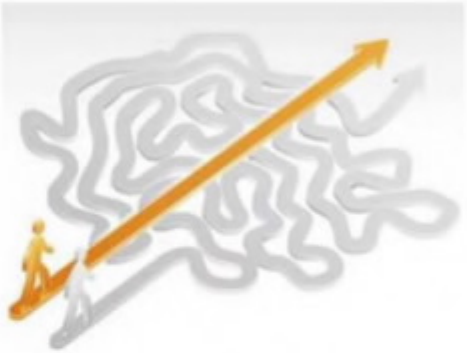
Solicitor-Client Privilege

s. 39 - Cabinet Confidence

Barring Interlocutory Appeals

Protected B

- Interlocutory appeal: an appeal of a judicial order during the trial, rather than waiting until the trial is over



- In NS context: appeal a disclosure or non-disclosure order (e.g. S. 38 privilege of sensitive information) of a designated judge to Federal or Supreme Courts during or before the criminal trial

- **Issue:** S. 38 litigation is complex and lengthy, and interlocutory appeals cause cascading delays as the trial is paused pending resolution of the disclosure litigation. Risks the *R v. Jordan* timeline

- **Proposal:** prohibit S. 38 interlocutory appeals until after successful conviction

Repealing Bifurcation

Protected B

- Bifurcation refers to the structure for adjudicating S.38 claims of NS privilege
- NS criminal trials are generally heard in provincial superior courts, but Federal Court (FC) has exclusive jurisdiction for adjudicating claims of NS privilege
- Thus, if a NS claim arises in a criminal trial taking place in superior court before a trial judge, that trial is paused while separate proceedings are held in the FC.

- **Issue:** bifurcation is complex and can lead to significant trial delays in prosecutions. Particularly problematic since *R v Jordan*.
- **Proposal:** amend S. 38 to provide jurisdiction to superior court trial judge to decide disclosure issues (similar to US, AUS systems)
- **Considerations:** Highly controversial. Advocates and detractors on both sides. Air India report supported. Solicitor Client Privilege. FC judges are well-trained in NS / S. 38, unlike SC judges, who also lack any secure infrastructure (major cost requirements)

Codifying Third Party Disclosure

Protected B

- *R. v. Stinchcombe* requires first parties, consisting of the prosecuting Crown (investigating police service and the prosecutor), to disclose all information in its possession that is not clearly irrelevant to the trial
- Third parties, such as CSIS, have much narrower – and no proactive – disclosure obligations (e.g. production of exculpatory records)
- However, *R v. O'Connor* requires the Crown to disclose 3rd party information that could reasonably be used by the accused to advance their defence. This is known as an *O'Connor* application; the prosecutor is also under a duty to make reasonable inquiries with GoC agencies to seek disclosure of information in their possession which may be relevant to the trial.

- **Issue:** O'Connor applications are regularly used as "fishing expeditions" to seek escalating production and review of CSIS information, which risks significant disclosure of sensitive information
- **Proposal:** legislate first and third party disclosure requirements to narrow third party obligations (e.g. threshold of "likely relevant" to a triable issue, third-party could first provide a summary of the information to the judge)

NS Justification for Sealing Warrants

Protected B

- When a warrant is executed, the authorization and supporting documents must be made public, unless the warrant is sealed by the issuing judge.
- S. 487.3 of the Criminal Code specifies that disclosure can be prevented based on a number of grounds, including a broad catch-all - "for any other sufficient reason"

- **Issue:** risk that the catch-all will not always cover NS grounds
- **Proposal:** create an express consideration to allow the sealing of warrants on the basis of injury to national security, defence, or international relations

- **Consideration:**

Solicitor Client Privilege

Solicitor Client Privilege

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Key Considerations

Protected B

- Of the reforms proposed by the panellists, many are promising but will require more thorough strategic policy and operational analysis to identify potential consequences or implementation requirements from the RCMP perspective.

- Of the additional legislative measures under consideration within the GoC, the RCMP is supportive of these reforms as they will very likely reduce the risk of violating *R v. Jordan* timelines and increase our ability to protect sensitive information.

- This will better enable the RCMP to collaborate with S&I partners and uphold public safety.

Discussion Questions for Experts

Protected B

- As noted, given the RCMP's role in NS investigations and the sensitivities associated with the vested interests of the experts, you will likely be in "listening mode" at tomorrow's meeting as it pertains to operational matters.

- However, there are key questions for you to ask from a policy perspective:
  - What benefits do the experts believe the 9 proposals would have, and what challenges or implementation requirements do they think would need to be resolved in order to effectively bring these changes into force?
  - What reforms do the experts feel should be explored first? Which would have the biggest impact for how NS prosecutions are carried out?
  - What precedence is there for some of these proposals – do any of them reflect lessons learned from other like-minded jurisdictions? (e.g. other Five Eyes don't have bifurcated process for adjudicating NS privilege claims).

Protected B

Questions?

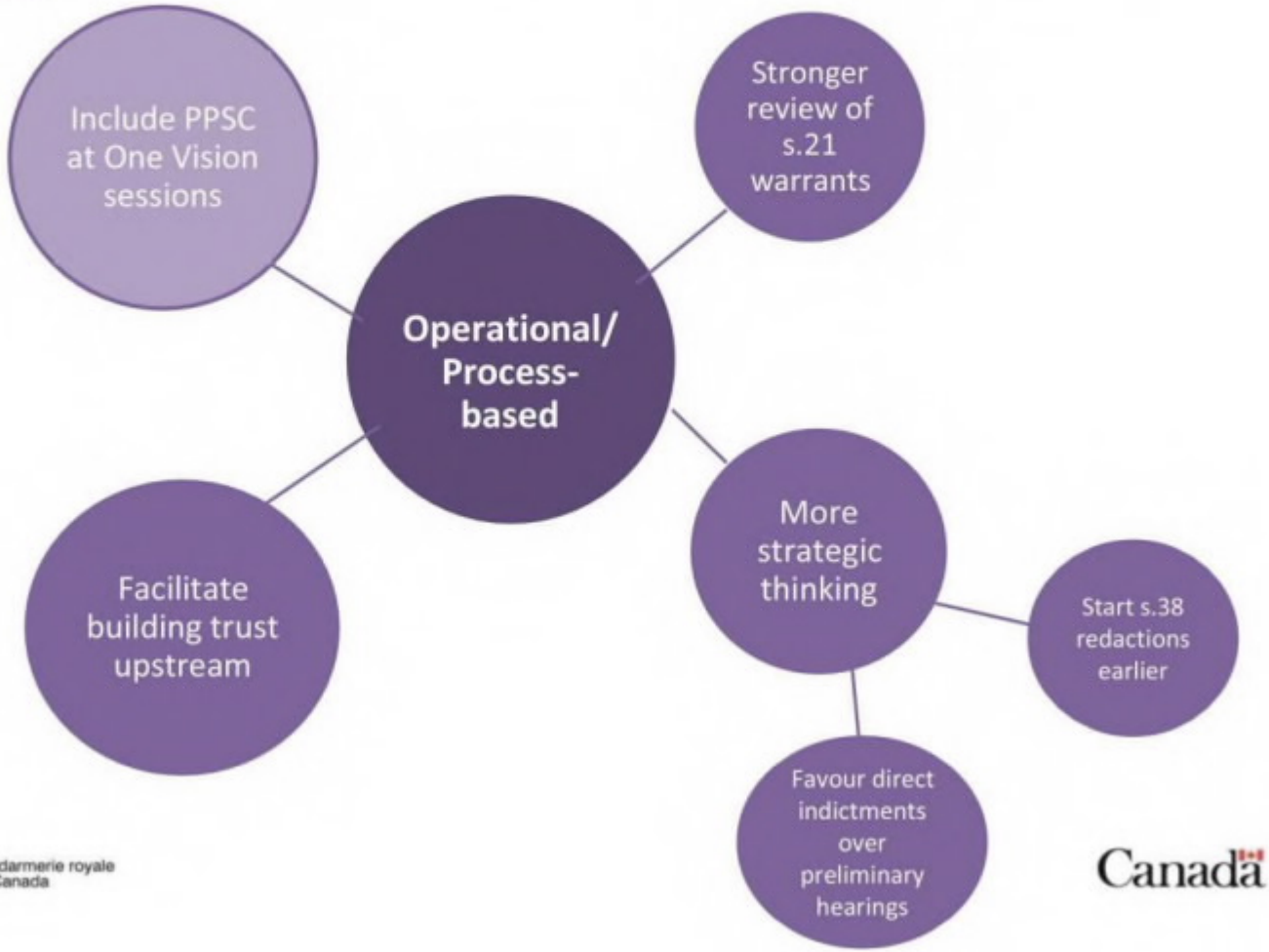
Canada

18

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Annex A: Key Issues (operational)

Protected B



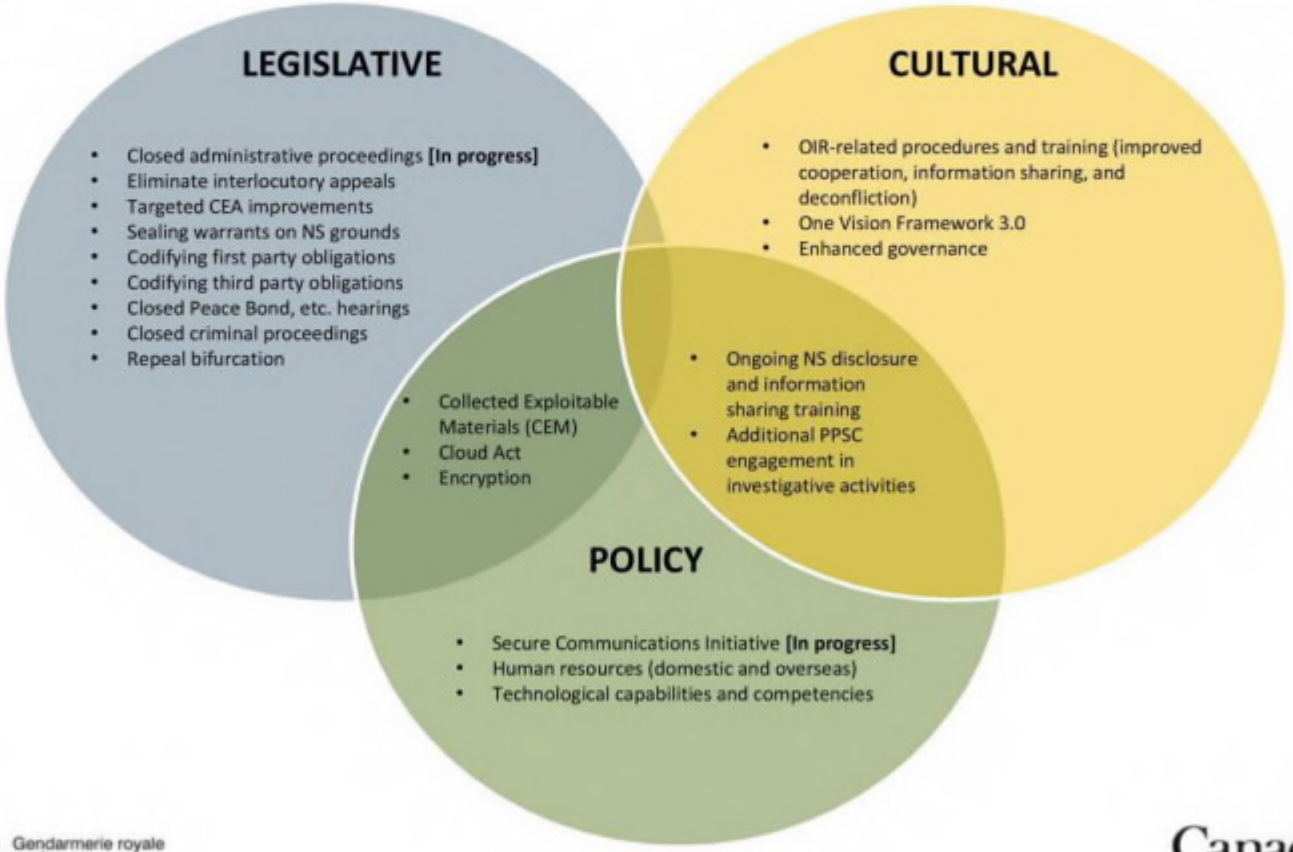
Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Annex B: I&E Efforts

Protected B

DN2



Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Slide 20

DN2

Moved slide 7 to the annex. Let me know if you disagree!

FP Strategic Policy, 4/3/2022 12:50:53 PM

Slide Notes

Slide 2:

On March 21, 2022, Public Safety hosted its second annual National Security Information- and Intelligence Sharing Symposium. The first panel was entitled "Canada's Intelligence and Evidence Model: The Way Forward".

During this panel, leading legal and academic experts familiar with the workings of Intelligence and Evidence (I&E) provided their perspectives on the evolution of the legal landscape since the Air India Commission of Inquiry and reviewed some of the key issues and challenges in this area.

Following the event, the PS and CSIS ADMs sought to organize a closed-door follow-up roundtable with the expert panellists to discuss legislative reform options. This meeting is taking place tomorrow, and you have been invited to represent the RCMP.

There was recognition that we, as policy makers, must reach out beyond the NS policy community to tap into the expertise of external stakeholders on the I&E dilemma if we are to find practical solutions to this issue.

On the panel, experts noted that the time has come to consider a "hard reset" of our approach, with the benefit of having now seen how it has played out and the number of issues associated with it.

Overall, the panel discussion pointed out that the pressure point seems to be the Service's insecurity over the control of its information, and that there also needs to be some more strategic thinking by Justice on s.38 matters; for example, if the Government does not intend to release the information, use of the AGC certificate may be preferable to multiple time-consuming appeals.

This pre-brief has been developed to prepare you for tomorrow's roundtable meeting.

Slide 4:

There are many occasions where CSIS intelligence, collected under its mandate, is shared with Government of Canada partners, especially the RCMP, to support its ability to carry out its law enforcement mandate. When the RCMP relies on this information to undertake enforcement action, the prosecuting Crown may be required to disclose CSIS intelligence in judicial proceedings.

When this occurs, the RCMP may be required to disclose CSIS intelligence in judicial proceedings. Often, that intelligence has been obtained from sensitive sources. This intelligence must be protected from public disclosure in order to prevent injury to CSIS' ability to carry out its investigations and in many cases, to protect people who have taken great risks to provide CSIS with critical national

security information. CSIS uses available measures in the current legal architecture to protect those people and that information from disclosure.

In some cases, information provided by CSIS to the RCMP cannot be disclosed and this can cause trial delays and other significant complications, including the potential staying of criminal charges: this is the intelligence and evidence challenge. Navigating this challenge to ensure effective collaboration between our two organizations while also upholding the rights of defendants and our disclosure obligations is a top priority for both the Commissioner of the RCMP and Director of CSIS. Both organizations have made significant improvements in the last several years to help resolve this challenge in the operational context, however, broader challenges remain.

There are significant structural issues which continue to undermine the GoC's ability to undertake effective NS investigations and carry out threat disruptions. Until these structural (i.e. legislative) issues are addressed, we will continue to operate with one hand tied behind our back in the NS space.

Slide 6:

Through the One Vision Framework and other operational efforts, the RCMP and CSIS have nearly exhausted available policy and operational reforms to address I&E challenges. To respond to remaining issues, legislative reforms need to be considered, and are imperative to address the overarching structural causes of the I&E challenge.

Extensive consideration of legislative change was conducted in 2018 and briefed to DMNS, but little progress has been made in terms of implementation.

Renewed commitment to exploring reform following several external reports and new Ministerial mandate.

There is also increasing recognition that the S&I and LE communities' ability to address existing or emerging NS threats (e.g. Canadian Extremist Travellers, etc.) is hampered until these long-standing issues are resolved.

Slide 8:

While this round-table was organized as a closed-door session, it is important to note that given the participants' interests and equities in this space, there will nevertheless remain a need for due diligence and care around the extent of any details provided that would speak to the RCMP's operational or investigative challenges that are not already available in the public domain.

The issues on this slide are those that were raised by the panellists during the NS Info-Sharing Symposium; of these, some are already under deliberation by the I&E Working Group and will be included in advice to the Minister on legislative reforms to meet his mandate commitment.
In particular, the proposal for closed Garofoli hearings and to codify 1st and 3rd party obligations.

For the remaining initiatives, it will be beneficial to glean a better sense from participants on what benefits they believe the 9 proposals would have, and inquire what challenges or implementation requirements they believe would need to be resolved in order to effectively bring these changes into force.
Discussion questions to this end have been included in slide 17.

Summaries of the 5 legislative proposals (summaries of the operational/process-based proposals are in Annex A):

Codify a third-party regime for records in prosecutions for national security offences, thereby limiting litigation around CSIS records, which is what causes the most uncertainty and fear.
In such a regime, there would be a duty on the Crown to make inquiries with CSIS to identify records that should be reviewed and assessed by the Crown for 'likely relevance'. If there is a reasonable possibility that the information is logically probative to an issue at trial or competence of a witness to testify, the information would be disclosable to the defense.
The regime would impose a very limited obligation on the defense to identify potential issues for trial that the Crown must consider when reviewing CSIS documents, which is essentially equivalent to what they have to do now. This would be consistent with obligation under O'Connor.
Once the Crown identified disclosable information in the Service's possession, they would be required to engage with the Service to determine the most appropriate way to provide the information to the accused in light of any applicable privileges. This could be done in various ways, including by redacting documents, providing summaries, admitting facts, drafting witness statements, etc.
In circumstances where information could not be produced because it would be injurious to international relationships, defence or security, or violate human source privilege, notice could then be given to the AGC. If the AGC does not permit it, then an in-camera ex parte hearing would be held with counsel from the AGC in the superior court, and if need be, special advocates could be appointed by the judge to advocate on behalf of the accused. The trial judge would then determine whether to order the disclosure of sensitive records, based on a test of injury to national security. The test would be as follows: Would the release of the information at issue cause injury to national security? If the answer is no, then the information must be disclosed. If injury is made out, then would the

disclosure be essential to trial fairness? If it is, then the Crown would have two options - either to disclose the information or seek a remedy by the trial judge.
If codifying a third-party regime, we would also need to look at potentially codifying additional protections for CSIS witnesses under s. 48(6) of the Criminal Code.

Codify a simpler s. 38 process to replace existing process, putting national security privilege on the same footing as informant privilege or solicitor/client privilege. The current process is overly complex. Although the s.38 process was subtracted from the Jordan timelines in Huang, being recognized as 'extraordinary steps', it doesn't leave a lot of room for ancillary motions, etc, within the context of a trial.

Modify the rule of automatic excision, which holds that constitutionally deficient information can't be relied upon in the context of a wiretap.

Close the Garofoli process with a special advocate.

Consider security-cleared defence counsel who would be able to make arguments on behalf of clients without disclosing the information (e.g. in informer cases). This could diffuse the litigation, with defence counsel seeing what is under the redactions.

Slide 12:
Considerations include:
No constitutional right to interlocutory appeal; would reduce Jordan risks; would require discussions about expanded use of AGC certificate; trial judge in Ader cited Jordan to refuse accused's attempt to make IA of section 38 order (useful precedent)

Slide 14:
For example, the accused could seek production and review of sensitive information used by CSIS to obtain section 21 warrants, the fruits of which are shared with the RCMP.

Slide 16:
In general, the reforms would make trials more timely, fair, and predictable for both the Crown and accused persons.

Could also add a point about confidence in our NS processes, both domestically and with international partners.

Slide 19:
Summaries of the 4 operational/process-based proposals:

Include prosecutors upstream, e.g. at One Vision sessions, to educate officials about the tools that the prosecutor has to protect information, in order to provide confidence that the Service can share information with the RCMP. There should be some comfort in the fact that core crucial investigative techniques will not be disclosed. [This is already underway through the One Vision process].

Facilitate building of trust and confidence upstream regarding control over information down the line, before prosecution. The UK is a good model for how prosecutors, law enforcement and national security investigators can effectively work together on information sharing. They created trust in the system and process through legislation and policy, so that the MI5 felt comfortable sharing information with prosecutors and criminal law enforcement, which allowed for the efficient use of intelligence in criminal investigations to protect public safety.

Create a more meaningful review of section 21 warrants and affidavit if in play in a criminal proceeding. Such a process would need to allow for a fair review of the warrants and underlying affidavits while ensuring that it is constitutionally sufficient. It remains to be seen whether these would be reviewed in the trial court or by the federal court, which would entail the federal court having jurisdiction to review its own warrants.

Apply more strategic thinking earlier, both at the operational and prosecutorial level. PPSC counsel would need to be mindful of timelines and ensure things are dealt with expeditiously.
Partners should start the actual section 38 redaction process as early on as possible, before charges are even laid if they can, and consult with relevant partners earlier (e.g. GAC).
We should favour direct indictment. In Huang, it was probably a strategic mistake to go with a preliminary hearing instead of moving to directly indict and get it into the court early on.

Slide 20:
This is a placemat currently under development by PS to outline for their Senior ADM (and potentially the Minister) the full gamut of I&E related initiatives.

The RCMP continues to engage with PS on the refining of this placemat.