

MEMORANDUM TO DIRECTOR GENERAL, POLICY AND FOREIGN RELATIONS

INTELLIGENCE AND EVIDENCE CHALLENGESISSUE:

To advise of existing challenges when intelligence is relied upon in support of criminal, administrative and civil proceedings.

BACKGROUND:

Proceedings are guided by key principles which require consistency with the *Charter of Rights and Freedoms* and respect for the Rule of Law. In accordance with the *Charter of Rights and Freedoms*, Canadians expect, and are generally guaranteed, procedural fairness, including open courts and transparent decision-making. There is, however, recognition that the Government has to protect sensitive sources, capabilities and techniques, as well as its relationships with foreign partners, in the interests of national security. The following mechanisms were created to enable the Government to protect sensitive information. Further details on these mechanisms are available in Annex 2.

- S.38 of the *Canada Evidence Act (CEA)*: Sets out a framework to reconcile, where possible, the Government's dual obligation of protecting national security and prosecuting the accused. Proceedings for which s.38 *CEA* is applied result in bifurcation of the Courts. For example, criminal proceedings are heard by trial judges in the provinces and s.38 *CEA* proceedings are heard in the Federal Court.
- S.18.1 of the *Canadian Security Intelligence (CSIS) Act*: Amongst other things, Bill C-44 amended the *CSIS Act*, with s.18.1 prohibiting the disclosure of the identity of a CSIS human source (or information from which it could be inferred), with very narrow exceptions.
- Division 9 of *IRPA*: Strengthens the Government's ability to keep those who pose a threat to the safety and security of Canada from entering and/or permanently residing in the country. Unlike s.38 *CEA*, sensitive information may be protected and relied upon under Division 9 of *IRPA*.
- *Prevention of Terrorist Travel Act (PTTA)*, *Secure Air Travel Act (SATA)*: Sensitive information may be considered and protected if its disclosure could be injurious to national security or endanger the safety of any person. While sensitive information may be withheld, the subject of the administrative decision would receive a summary of the information used to make the decision.

DISCUSSION:

Despite mechanisms to protect sensitive information, litigation involving issues of national security often results in lengthy legal processes that are resource intensive and that jeopardize national security through the production and disclosure of sensitive information.

Beyond the considerable financial resources required to support these cases, the production and disclosure of sensitive information also entails a substantial risk to national security. While the aforementioned provisions provide for the protection of classified information in s.38 *CEA* proceedings, the Court may decide that disclosure is required if the public interest outweighs its protection. As a result, numerous disclosures have and continue to be made concerning CSIS investigative interests, tradecraft, human

source operations and information provided by foreign partners. These disclosures negatively impact CSIS operations and adversely affect Canada's national security interests.

In criminal proceedings, CSIS may, after charges are laid, be required to disclose classified information when information is deemed relevant under the *Stinchcombe*¹ standard of disclosure, as well as when it is held by CSIS as a third party, is 'likely relevant' to an issue and an application for disclosure has been made. CSIS may also be required to disclose such information when it is determined that, as part of a s.38 *CEA* proceeding, a balancing of public interests favours disclosure. Reliance on CSIS information as evidence in criminal proceedings will either result in public disclosure of that information or its protection, ultimately weakening the Government's ability to continue the proceedings or, in some cases, pursue charges.

Litigation also has the potential to adversely impact the Government's national security policy objectives and ability to effectively administer and enforce laws. For instance, where no specific regime is in place (e.g. *Investment Canada Act*, listings, exports, etc.), a wide range of administrative decisions must rely on s.38 *CEA* to protect sensitive information. If protected, that information may not be relied upon, weakening the Government's ability to defend its case. In addition, while sensitive information may be relied upon under Division 9 of *IRPA*, disclosure obligations from past decisions have rendered these proceedings complex, lengthy and costly while also requiring CSIS to produce an unprecedented amount of sensitive information to the Court and special advocates.

Finally, in civil proceedings, the Government does not have control over the civil suits it is brought into. Once brought into a proceeding, the Government, when it is unable to rely on undisclosed CSIS information to mount its defence, must choose between settling the case or disclosing sensitive information. Notwithstanding the damage to the Government's reputation, this also has significant monetary implications for the Government.

CONCLUSION:

Intelligence and evidence has also been included in forthcoming consultations on national security issues and the related Green Paper. Public feedback resulting from these consultations may assist in guiding reform on the issue, particularly as it relates to maintaining balance between trial fairness and the protection of national security information.

The above processes do not include immediate solutions to issues associated with intelligence and evidence. As such, to mitigate such issues, the Service has, with its partners, created a whole range of processes to protect classified information that may be used to inform enforcement actions. For instance, the *One Vision* framework for cooperation between CSIS and the Royal Canadian Mounted Police (RCMP) was enhanced to avoid inadvertent disclosure of CSIS information to RCMP. This, given that information shared with the RCMP may appear in their case files, judicial authorisations and disclosure packages to the Court as part of criminal prosecutions, ultimately becoming subject to disclosure obligations.

¹ In criminal cases, the accused has a constitutional right to full and complete disclosure of the Crown's case. The Crown is therefore obliged to disclose all relevant (or, not clearly irrelevant) information in its possession.



INTELLIGENCE AND EVIDENCE

BRIEF TO THE PRIVY COUNCIL OFFICE

SECRET



WEDNESDAY, 4 MAY 2016

Canada

PURPOSE

SECRET

- ☐ To provide an overview of key issues related to the increased demand for CSIS to produce and/or disclose intelligence in support of administrative, civil or criminal proceedings.

CURRENT CONTEXT

SECRET

- ☐ CSIS collects information and intelligence
 - threshold for investigation: reasonable grounds to suspect
 - rely on sensitive sources and methods, foreign partner information
 - complex, inter-related investigations
- ☐ Mandate to advise government, and to provide security advice and assessments
 - CSIS intelligence informs or is relied upon by GoC in support of administration or enforcement of laws, including criminal investigations
- ☐ Increased cooperation between departments has resulted in an increasing number of proceedings involving CSIS information
- ☐ Sheer number of proceedings, coupled with expanded disclosure obligations jeopardizes the integrity of CSIS operations and ultimately, the ability of CSIS to fulfill its mandate

KEY CONSIDERATIONS

SECRET

- ☐ The goal is to achieve successful outcomes in the administration and enforcement of Canadian law in a manner that:
 - respects the principles of fundamental justice
 - protects sensitive sources and techniques, as well as relationships with foreign partners

- ☐ Currently rely on a number of mechanisms to manage intelligence in civil, criminal and administrative proceedings
 - Canada Evidence Act (s.38), CSIS Act (s.18.1), Immigration and Refugee Protection Act (Division 9), Prevention of Terrorist Travel Act and Secure Air Travel Act

- ☐ Each regime is unique. Key distinctions include:
 - Bifurcation (Protection of intelligence versus protection and reliance on intelligence)
 - Balancing of injury against public interest versus no-balancing

CANADA EVIDENCE ACT (CEA)

SECRET

- ☐ Where no other mechanism exists, Section 38 of the CEA is relied upon
 - if Federal Court judge determines injury outweighs public interest in disclosure, intelligence is protected, but may not be relied upon by the trier of fact
- ☐ Bifurcation and balancing pose a number of challenges.
 - bifurcated process is costly and significantly delays document production
 - balancing of national security and public interest creates uncertainty
 - if protected, weakens Government's ability to defend its case; undisclosed information not seen the trial judge, weight given to summary not certain
 - if ordered disclosed, must choose to either publicly disclose classified intelligence or withdraw case/settle

APPLICATION OF CEA

SECRET

CIVIL PROCEEDINGS

- ☐ No Government control over the number of new civil suits

CRIMINAL PROCEEDINGS

- ☐ Extensive disclosure obligations; few exceptions to the accused's right to know the case against them (innocence at stake)

ADMINISTRATIVE PROCEEDINGS

- ☐ Where no specific regime in place, judicial review of wide range of administrative decisions must rely on CEA; not a robust system for the administration of laws

IMMIGRATION AND REFUGEE PROTECTION ACT (IRPA)

SECRET

- ☐ Division 9 of IRPA allows for the protection of and reliance on intelligence in determining the admissibility of foreign nationals to Canada
 - relies on open and closed proceedings
 - all information disclosed in closed proceedings, including to special advocates (SAs)
 - no balancing; if judge injurious to national security, information is protected
- ☐ Notwithstanding amendments, regime continues to face challenges
 - disclosure obligations from past decisions result in complex, costly and lengthy proceedings
 - unprecedented amount of classified information disclosed to the Court, SAs, defence
- ☐
 - one certificate withdrawn (Charkaoui), ongoing appeals to Supreme Court

STEPS TAKEN

SECRET

- ☐ CSIS carefully manages disclosure to partners and continues to adapt internal protocols (One Vision,)
- ☐ Series of legislative initiatives
 - Bill C-44: Class privilege for human sources
 - *Secure Air Travel Act, Prevention of Terrorist Travel Act*: specific provisions for judicial review and appeal, to permit judges to rely on and protect classified information
- ☐ Actively engaged in policy work led by the Department of Justice to develop proposals for reform (civil, criminal and administrative)

CONCLUSION

SECRET

- ☐ CSIS continues to work closely with partners to support the effective administration and enforcement of laws, notwithstanding the significant risks associated with public disclosure of CSIS intelligence and methods
- ☐ Would welcome opportunity to bring forward proposals for reform



Canada

- 
- ☐ To provide an overview of key issues related to the increased demand for CSIS to produce and/or disclose intelligence in support of administrative, civil and criminal proceedings.
- 

☐ CSIS collects information and intelligence

- threshold for investigation: reasonable grounds to suspect
- rely on sensitive sources and methods, foreign partner information
- complex, inter-related investigations

☐ Mandate to advise government, and to provide security advice and assessments

- CSIS intelligence informs or is relied upon by GoC in support of administration or enforcement of laws, including criminal investigations

☐ Increased cooperation between departments has resulted in an increasing number of proceedings involving CSIS information

☐ Sheer number of proceedings, coupled with expanded disclosure obligations jeopardizes the integrity of CSIS operations and ultimately, the ability of CSIS to fulfill its mandate

- 
- ☐ The goal is to achieve successful outcomes in the administration and enforcement of Canadian law in a manner that:
 - respects the principles of fundamental justice
 - protects sensitive sources and techniques, as well as relationships with foreign partners
 - ☐ Currently rely on a number of mechanisms to manage intelligence in civil, criminal and administrative proceedings
 - Canada Evidence Act (s.38), CSIS Act (s.18.1), Immigration and Refugee Protection Act (Division 9), Prevention of Terrorist Travel Act and Secure Air Travel Act
 - ☐ Each regime is unique. Key distinctions include:
 - Bifurcation (Protection of intelligence versus protection and reliance on intelligence)
 - Balancing of injury against public interest versus no-balancing
- 



☐ Where no other mechanism exists, Section 38 of the *CEA* is relied upon

- if Federal Court judge determines injury outweighs public interest in disclosure, intelligence is protected, but may not be relied upon by the trier of fact

☐ Bifurcation and balancing pose a number of challenges.

- bifurcated process is costly and significantly delays document production
 - balancing of national security and public interest creates uncertainty
 - if protected, weakens Government's ability to defend its case; undisclosed information not seen the trial judge, weight given to summary not certain
 - if ordered disclosed, must choose to either publicly disclose classified intelligence or withdraw case/settle
- 



CIVIL PROCEEDINGS

- ☐ No Government control over the number of new civil suits

CRIMINAL PROCEEDINGS

- ☐ Extensive disclosure obligations; few exceptions to the accused's right to know the case against them (innocence at stake)

ADMINISTRATIVE PROCEEDINGS

- ☐ Where no specific regime in place, judicial review of wide range of administrative decisions must rely on CEA; not a robust system for the administration of laws
- 



☐ Division 9 of IRPA allows for the protection of and reliance on intelligence in determining the admissibility of foreign nationals to Canada

- relies on open and closed proceedings
- all information disclosed in closed proceedings, including to special advocates (SAs)
- no balancing; if determined injurious to national security, information is protected

☐ Notwithstanding amendments, regime continues to face challenges

- disclosure obligations from past decisions result in complex, costly and lengthy proceedings
- unprecedented amount of classified information disclosed to the Court, SAs, defence

☐

- Lengthy litigation process, certificates nullified (Charkaoui) or deemed unreasonable (Almrei) resulting in ongoing civil proceedings
- 



☐ CSIS carefully manages disclosure to partners and continues to adapt internal protocols (One Vision,)

☐ Series of legislative initiatives

- Bill C-44: Class privilege for human sources
- *Secure Air Travel Act, Prevention of Terrorist Travel Act*: specific provisions for judicial review and appeal, to permit judges to rely on and protect classified information

☐ Actively engaged in policy work led by the Department of Justice to develop proposals for reform (civil, criminal and administrative)



☒ CSIS continues to work closely with partners to support the effective administration and enforcement of laws, notwithstanding the significant risks associated with public disclosure of CSIS intelligence and methods

☐ Would welcome opportunity to bring forward proposals for reform

Committee Note

INTELLIGENCE AND EVIDENCE

ISSUE: Why is intelligence appearing in judicial proceedings? What are issues associated with the reliance on intelligence as evidence? Are there not existing authorities that protect the release of sensitive information?

- As the Service's mandate is to investigate threats to the security of Canada and provide related advice to the Government of Canada, CSIS frequently shares threat-related information with other government departments.
- CSIS information may therefore inform or be relied upon by the Government in support of the administration or enforcement of laws.
- The result, however, is that CSIS intelligence is often drawn into public proceedings – civil, criminal or administrative.
- The intent is to protect national security information while ensuring decision-makers have access to relevant information.
- If released publicly, sensitive information like this could compromise intelligence operations, the safety of CSIS sources, CSIS capabilities and techniques and Canada's relationships with foreign partners.
- It is therefore essential for the Service to protect this information against public disclosure using available legal tools, as appropriate.

IF PRESSED ON EXISTING AUTHORITIES TO PROTECT SENSITIVE INFORMATION:

- A number of mechanisms are relied upon to manage sensitive information in legal proceedings.
- Section 38 of the *Canada Evidence Act* provides for the protection of sensitive information when national security is at risk.
- The *CSIS Act* was recently amended to include s.18.1, which provides greater protection for human sources.
- Under Division 9 of the *Immigration and Refugee Protection Act*, sensitive information may be protected and relied upon to prevent those who pose a threat to the safety and security of Canada from entering and/or permanently residing in the country.
- Under the *Prevention of Terrorist Travel Act*, sensitive information may be protected and considered during judicial review of our Minister's decision to refuse or revoke a passport for national security purposes, or during appeal of the decision to cancel a passport for those purposes.
- Sensitive information may also be protected and considered under the *Secure Air Travel Act*, when individuals appeal the Minister's decision to add persons to Canada's "no-fly list" or to direct air carriers to deny transportation or perform additional screening of a person.
- When the Service's sensitive information is ordered to be disclosed, CSIS

must weigh the operational cost of disclosing such information against the benefit of a potential prosecution.

- A decision to withdraw information could put the case in jeopardy.

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

Committee Note
INTELLIGENCE AND EVIDENCE

ISSUE: Why is intelligence appearing in judicial proceedings? What are issues associated with the reliance on intelligence as evidence? Are there not existing authorities that protect the release of sensitive information?

- **As the Service's mandate is to investigate threats to the security of Canada and provide related advice to the Government of Canada, CSIS frequently shares threat-related information with other government departments.**
- **The intent is to protect national security information by ensuring decision-makers have access to relevant information,**
- **The result, however, is that CSIS intelligence is drawn into public proceedings – civil, criminal or administrative.**
- **If released publicly, this information could compromise: intelligence operations, the safety of CSIS sources, CSIS capabilities and techniques and Canada's relationships with foreign partners.**
- **It is therefore essential for the Service to protect this information against public disclosure using available legal tools, as appropriate.**

IF PRESSED ON EXISTING AUTHORITIES TO PROTECT SENSITIVE INFORMATION:

- **Section 38 of the *Canada Evidence Act* provides for the protection of sensitive information when national security is at risk.**
- **The *CSIS Act* was also amended to include s.18.1, which provides greater certainty in relation to the protection of the identity of human sources.**
- **When the Service's sensitive information cannot be protected, the Service must make a decision as to whether or not that information should be withdrawn from the case. In doing so, it must weigh the operational cost of disclosing such information against the benefit of a potential prosecution.**

Committee Note

INTELLIGENCE AND EVIDENCE

ISSUE: Why is intelligence appearing in judicial proceedings? What are issues associated with the reliance on intelligence as evidence? Are there not existing authorities that protect the release of sensitive information?

- As the Service's mandate is to investigate threats to the security of Canada and provide related advice to the Government of Canada, CSIS frequently shares threat-related information with other government departments.
- The intent is to protect national security information by ensuring decision-makers have access to relevant information,
- The result, however, is that CSIS intelligence is drawn into public proceedings – civil, criminal or administrative.
- If released publicly, this information could compromise: intelligence operations, the safety of CSIS sources, CSIS capabilities and techniques and Canada's relationships with foreign partners.
- It is therefore essential for the Service to protect this information against public disclosure using available legal tools, as appropriate.

IF PRESSED ON EXISTING AUTHORITIES TO PROTECT SENSITIVE INFORMATION:

- Section 38 of the *Canada Evidence Act* provides for the protection of sensitive information when national security is at risk.
- The *CSIS Act* was also amended to include s.18.1, which provides greater certainty in relation to the protection of the identity of human sources.
- When the Service's sensitive information cannot be protected, the Service must make a decision as to whether or not that information should be withdrawn from the case. In doing so, it must weigh the operational cost of disclosing such information against the benefit of a potential prosecution.

Committee Note

INTELLIGENCE TO EVIDENCE

ISSUE: Why is intelligence appearing in judicial proceedings? What are issues associated with the reliance on intelligence as evidence? Are there not existing authorities that protect the release of sensitive information?

IF PRESSED ON INTELLIGENCE AND EVIDENCE

- As the Service's mandate is to investigate threats to the security of Canada and provide related advice to the Government of Canada, CSIS frequently shares threat-related information with other government departments.
- The intent is to protect national security information by ensuring decision-makers have access to relevant information,
- The result, however, is that CSIS intelligence is drawn into public proceedings – civil, criminal or administrative.
- If released publicly, this information could compromise: intelligence operations, the safety of CSIS sources, CSIS capabilities and techniques and Canada's relationships with foreign partners.
- It is therefore essential for the Service to protect this information against public disclosure using available legal tools, as appropriate.

IF PRESSED ON EXISTING AUTHORITIES TO PROTECT SENSITIVE INFORMATION:

- Section 38 of the *Canada Evidence Act* provides for the protection of sensitive information when national security is at risk.
- The *CSIS Act* was also amended to include s.18.1, which provides greater certainty in relation to the protection of the identity of human sources.
- When the Service's sensitive information cannot be protected, the Service must make a decision as to whether or not that information should be withdrawn from the case. In doing so, it must weigh the operational cost of disclosing such information against the benefit of a potential prosecution.