~~TOP SECRET // CEO~~

~~SOLICITOR CLIENT PRIVILEGE~~

Rebuilding Trust:

Reforming the CSIS Warrant and Justice Legal Advisory Processes

NSIRA Review arising from Federal Court's Judgment in 2020 FC 616

NSIRA REVIEW 21-18

I EXECUTIVE SUMMARY 3

II AUTHORITIES 12

III INTRODUCTION 12

A. REVIEW BACKGROUND 13
B. METHODOLOGY 14
C. INSTITUTIONAL ENVIRONMENT 16
1. Systemic, Governance and Cultural Issues 16
2. Legal and Operational Structures 17
a. CSIS 17
b. Justice and NSLAG 18

IV ANALYSIS 20

A. JUSTICE'S PROVISION OF LEGAL ADVICE 20
1. Giving Advice to CSIS 20
a. Obtaining Advice 22
b. The Nature of the Legal Advice 23
2. Reform Initiatives 26
a. NSLAG's Recent Internal Protocols 26
b. Renewed NSLAG and CSIS Relations 27
c. Additional Steps at NSLAG 29
d. Broader Department of Justice 30
B. WARRANT PROCESS 35
1. Basic Legal Rules 35
2. Historical Initiatives 37
3. Description of the Warrant Process 37
a. Prioritization of Investigations for Warrants 38
b. The Complexity of the Warrant Acquisition Process 39
c. The Key Steps in the Process 40
4. Observations on the Warrant Process 41
a. A Lengthy, Bureaucratic Process 41
b. Incomplete Knowledge Management in the Regions 45
i. Misunderstanding Concepts 45
ii. Information Management Struggles 47
iii. Fixing the Recurring Omissions Problem 48
c. The Affiant Unit 50
i. The Traditional Approach 50
ii. The Current Approach 50
iii. The Advantages of an Affiant Unit 51
iv. Challenges to Affiant Unit Sustainability 52
v. Improving and rebuilding 53
d. NSLAG Warrants Counsel 56
e. Revamping the Independent Challenge Function 58
i. The Imperfect Independent Counsel Model 58
ii. Reconceiving Public Safety's Oversight Role 61
f. Submission to the Federal Court 63
g. Doubts Arising on Warrant Execution 64
C. INVESTMENT IN PEOPLE: TRAINING 65

V. CONSEQUENCES OF SYSTEMIC PROBLEMS 67

A. Morale and Cultural Resistance to Change 67
B. Performing the mission 69

ANNEX A: HISTORICAL INITIATIVES 73
ANNEX B: WARRANTS ACQUISITION SCHEDULE: 91
ANNEX C: AFFIANT BRANCH ORGANIZATIONAL STRUCTURE 95

I EXECUTIVE SUMMARY

This is a report about the manner in which the Canadian Security Intelligence Service (CSIS) seeks and receives legal services from the Department of Justice (Justice) and prepares and executes the warrants it needs to collect information. This review stemmed from a 2020 decision of the Federal Court (2020 FC 616). In that matter, the Federal Court recommended that a "comprehensive external review be initiated to fully identify systemic, governance and cultural shortcomings and failures that resulted in CSIS engaging in operational activity that it has conceded was illegal and the resultant breach of candour."

This review found an intelligence service and its counsel who struggle to organize themselves in a manner that allows them to meet easily their legal obligations, including to the Federal Court. NSIRA also found a failure at CSIS to professionalize fully and sustainably the warrant application process as a specialized trade that requires training, experience, and investment. This report also demonstrates the need to transform the relationship between CSIS and its legal counsel.

This review was led by NSIRA Members Marie Deschamps and Craig Forcese. One or both Members were directly involved in every aspect of the review including review process management, briefings, interviews and document review. To conduct this review, NSIRA conducted dozens of confidential interviews with Justice and CSIS employees whose perspectives were essential for "ground-truthing" the knowledge NSIRA had gained from documents and formal briefings. In organizing these interviews, NSIRA ensured robust representation covering the range of functions in the warrant and legal-advice giving processes. The interviews raised issues and concerns that would have otherwise been unavailable to NSIRA. This assisted NSIRA in making recommendations on governance, systemic, and cultural issues that contribute to inefficiencies threatening the ability of CSIS and Justice to fulfil their mandates.

NSIRA heard repeated concerns from interviewees that the problems stemming from governance, systemic, and cultural challenges put at risk the ability of the intelligence service to meet the mandate Parliament has assigned to it. Addressing these challenges is in the urgent public interest. Though CSIS and Justice have made improvements, difficulties are still evident.

NSIRA groups its findings and recommendations into three overarching areas:

A. Justice's Provision of Legal Advice
B. CSIS's and Justice's Management of the Warrant Acquisition Process
C. Investment in People

In its conclusion, this report also makes comments and recommendations about the broader cultural and governance context.

Justice's Provision of Legal Advice

CSIS operates in often rapidly evolving and legally challenging environments. Timely, nimble and actionable legal advice is critical. This review highlighted factors that prevent the National Security Litigation and Advisory Group (NSLAG) of Justice from providing CSIS with the operational advice it needs.

Justice has employed a centralized "one voice" model for delivering its legal services. The "one voice" model reflects a desire for uniform and consistent legal advice delivered on behalf of the Attorney General of Canada. Although the premise for the "one voice" approach is sound, NSIRA found that NSLAG struggled to provide timely, responsive, and useful legal advice in the CSIS

context. The way Justice provides advice has often not been responsive to CSIS operations. For example, NSLAG presents its advice as a legal risk assessment using the Justice-wide Legal Risk Management grid. This grid uses a colour-coded risk rating that can be compared to a "traffic light" system: a green risk rating represents a low legal risk to CSIS, a red risk rating represents a high legal risk, and, more ambiguously, a yellow risk rating represents an intermediate legal risk. Yellow light responses are reportedly the most common and the most frustrating for CSIS, especially when unaccompanied by discussions on how to mitigate the risk, the inclusion of which NSIRA heard is not currently common practice.

In consequence, some at CSIS perceive Justice as presenting a road-block because of its bureaucracy, its perceived operational illiteracy, and its unhelpful approach to communicating legal advice.

However, the problems with timely, responsive, and useful legal advice do not stem from Justice alone. NSIRA heard that CSIS has not always shared all relevant information with Justice, prompting a degree of mistrust. The internal process for requesting legal advice at CSIS also contributes to delays and lack of relevance. The advice that sometimes comes back to operational investigators at CSIS filtered through bureaucratic hierarchies may be of limited or little relevance.

NSIRA heard that the laborious advice-seeking and -receiving process has sometimes caused [redacted] [discussion of the detrimental effects on and risks to operations] [redacted]

CSIS and Justice often operate in a situation of legal doubt, because of lack of clarity in the law. Clarifying legal standards often requires judicial case law. However, an unwieldy warrant process, discussed below, makes that prospect more difficult.

Finding no. 1: NSIRA finds that the legal advice-seeking and giving process, and resource constraints at NSLAG contribute to considerable delays, [description of timeline] [redacted]

Finding no. 2: NSIRA finds that Justice legal opinions have sometimes been prepared without sufficient attention to the audience that needs to understand and act on them. Opinions have been focused on assessing legal risk, often late in the development of a CSIS activity, with limited effort made to propose alternative and legally sustainable means of arriving at the intended objective.

Finding no. 3: NSIRA finds that the Justice Legal Risk Management Framework is misunderstood at the working level at CSIS and further that it does not provide an appropriate framework for the unequivocal communication of unlawful conduct to CSIS.

Finding no. 4: NSIRA finds that difficulties in acquiring prompt and relevant legal advice have contributed to [discussion of the detrimental effects on and risks to operations] [redacted] **that may require legal advice. In consequence, the manner in which Justice has provided legal advice to CSIS does not always meet the needs of CSIS operations.**

Finding no. 5: NSIRA finds that Justice does not generate the necessary business analytics to track its service delivery performance to CSIS.

Justice is aware of the need for change. Broad, recent initiatives include the Vision Project, which promises client-centric strategic partnerships. New procedures have been implemented at NSLAG to address internal silos between advisory and litigation counsel, and to improve training, access to legal advice and facilitate consistent legal opinions. NSLAG also appears to recognize the desire for a different approach to providing legal advice, including moving toward legal advice that promotes collaborative and iterative engagement with CSIS to achieve its operational goals, within

the bounds of the law (a "road map"-style form of advice-giving). However, it does not appear that CSIS and Justice have thus far systematically put this model into effect.

To facilitate proper advice-giving, especially in a "road map"-style model, CSIS needs to provide NSLAG with all the facts, and to engage NSLAG early on, at the operational level. Earlier and ongoing involvement throughout the stages of an investigation or operation would enable counsel to provide informal legal nudges that allow CSIS to course-correct before too much time has been spent. A more iterative process of incorporating legal advice over the full course of an operation could address the reported challenge of operations halted due to untimely or ambiguous legal advice.

Finding no. 6: NSIRA finds that Justice has acknowledged that internal silos at NSLAG between the advisory and litigation wings have sometimes left warrant counsel unaware of emerging legal issues and that Justice has taken steps to resolve these issues.

Finding no. 7: NSIRA finds that Justice has committed to improve its advice-giving to CSIS, including moving toward "road map" style legal advice that involves working collaboratively and iteratively with CSIS to achieve operational goals within the bounds of the law.

Finding no. 8: NSIRA finds that CSIS has not always shared all relevant information with NSLAG, prompting a degree of mistrust and limiting Justice's ability to provide responsive legal advice.

In view of these findings, NSIRA recommends that:

Recommendation no. 1: Justice pursue its commitment to reforming the manner of providing legal advice to CSIS, and its stated commitment to "road map"-style advice as a best practice. In support of this objective and the provision of timely, operationally relevant advice, NSIRA further recommends that Justice implement the following:

- **Whether through an expanded "office hours" and liaison counsel program or otherwise, NSLAG must develop a legal support service operating full time, staffed by experienced lawyers empowered to provide operational advice in real time on which CSIS officers can rely, on the basis of settled Justice positions on recurring legal issues, accessible directly to CSIS officers across all regional offices and at all levels.**

- **NSLAG develop a concise reference tool with its position on recurring issues and most common legal authorities invoked and make the tool accessible to counsel to support their real-time advice.**

- **To minimize the need to resort to the formalized legal advice-seeking process, NSLAG (in coordination with CSIS) must involve counsel with CSIS officers at the early stage of the planning of key or novel operations and throughout their entire operational lifecycle to case-manage an iterative legal guidance process.**

Recommendation no. 2: NSLAG (in coordination with CSIS) develop Key Performance Indicators to measure the delivery of legal services to CSIS.

Recommendation no. 3: CSIS and Justice include in their training programs interactive scenario-based training developing the operational intelligence activities expertise of NSLAG counsel and the legal knowledge of CSIS operational staff.

Recommendation no. 4: To ensure Justice is able to give meaningful and responsive legal advice as recommended in recommendation #1, CSIS invite Justice counsel to sit at the table at all stages of the lifecycle of key and novel operations, and that it fully and frankly brief counsel on operational objectives, intent, and details.

Recommendation no. 5: Justice's advice-giving must clearly and unequivocally communicate advice on the unlawfulness of client conduct, whether criminal or otherwise.

Management of the Warrant Process

CSIS organizes the process of seeking a warrant around a system of internal preparation and approvals before proceeding to the statutory step of seeking ministerial approval of the warrant application. A number of legal concepts and expectations enter into the warrant process, including the "duty of candour" owed to the Court.

The Federal Court duty of candour concerns now fit into two categories: disclosure of information material to the credibility of the sources who supply information used in the application; and disclosure of information material to matters of potential concern about the broader context of the warrant and how it will be executed.

Despite past attempts at reforms the current warrant process adopted by CSIS and supported by Justice, the warrant process has repeatedly failed to meet these candour obligations. Many reforms appear to have contributed to the bureaucratic complexity of the warrant process, without addressing candour issues.

Finding no. 9: NSIRA finds that CSIS has a history of quick reforms, followed by neglect, high turnover of personnel leading to a loss of institutional knowledge, and resourcing that did not match stated priorities. CSIS does not track or measure the outcome of past reforms adequately and has no performance metrics for assessing success.

Finding no. 10: NSIRA finds that CSIS policies have not kept pace with operational reality, as they are often vague, dated, overlapping and contradictory. The absence of clear policy creates legal doubt or concerns, and gives rise to disparate interpretations of legal and operational standards.

Finding no. 11: NSIRA finds that there is little common understanding regarding the process or basis on which a warrant is prioritized. Frequent shifts in this process of prioritization have added to operational uncertainty. The prioritization process has made it very difficult to bring novel issues to the Court with the goal of addressing legal ambiguities through court decisions.

Finding no.12: NSIRA finds that the actors involved in the warrant process do not have a common understanding of the rationale for each of the [multiple] of steps in the overarching warrant application scheme and are not always sure what role each approval step plays.

Finding no. 13: NSIRA finds that the proliferation of process in seeking warrants has created a system of diluted accountability widely regarded as slow and unwieldy, with delays caused by multiple levels of approval.

Finding no. 14: NSIRA finds that there is no regular feedback process in which explanations for warrant-related decisions made at one level filter back to other levels. The absence of feedback is especially acute for the regional investigators.

Finding no. 15: NSIRA finds that often, the sole means to address legal uncertainty is to bring legal questions to the Federal Court through warrant applications. In consequence, an unwieldy warrant process makes resolution of legal doubt more difficult.

CSIS has struggled especially to ensure that all information material to the credibility of sources is properly included in warrant applications. NSIRA heard repeatedly that CSIS officers involved in the early stages of preparing warrant applications do not clearly understand the legal expectations surrounding the duty of candour. Deficient information management systems related to human sources at CSIS have also resulted in important omissions, violating duty of candour obligations. These challenges produce what NSIRA calls the "recurring omissions" problem.

Finding no. 16: NSIRA finds that CSIS has struggled to ensure that all information material to the credibility of sources is properly contained in warrant applications. This "recurring omissions" problem stems from a misunderstanding of the Federal Court's role in assessing the credibility of sources and from the presence of multiple, siloed information management systems. NSIRA acknowledges that CSIS has undertaken reforms, but work remains to implement successfully long term sustainable solutions.

In view of these findings, NSIRA recommends that:

Recommendation no. 6: CSIS adopt, and share internally, clear criteria for the warrant prioritization process.

Recommendation no. 7: CSIS establish a new warrant process eliminating steps that do not make a significant contribution to a more accurate application. The process should assign clear lines of responsibility for the production of accurate applications. The reformed system should ensure that delays associated with managerial approvals are minimized, and that time is reallocated to those steps contributing to the preparation of the accurate applications.

Recommendation no. 8: CSIS integrate the regional stakeholders (including the implicated investigators) at every key milestone of the warrants process.

Recommendation no. 9: CSIS adopt policies and procedures governing the reformed warrant process that clearly outlines the roles and responsibilities of each participant and the objective of each step in the warrant process and that these policies be kept current as the process evolves.

Recommendation no. 10: To address the seeming inevitability of "recurring omissions", NSIRA recommends that CSIS prioritize the development of [an improved] system for human source information management. CSIS should also continue initiatives meant to ensure that source handlers are assiduous in documenting and then reporting in source precis information going to credibility. Even with these reforms, the Affiant Unit should adopt procedures for verifying the information prepared by the regions.

In 2019, CSIS sought to professionalize affiant work by creating an Affiant Unit (AU). CSIS's establishment of the AU is a critical development and, properly resourced and staffed, it would be well positioned to respond to long-standing problems with the duty of candour. However, when created, the AU was placed under the [Name of Branch]. [Name] has a broad mandate that does not align with the AU's functions in preparing legally robust warrant applications. This governance anomaly may explain the AU's present administrative and human resource challenges. The AU's sustainability is in question, and indeed NSIRA heard that the unit could currently be described as in a state of crisis. CSIS has not supported the unit with resources commensurate with the importance of this unit in fulfilling CSIS's mission.

Finding no. 17: NSIRA finds that the Affiant Unit (AU) constitutes a vital and laudable reform within CSIS. However, the AU is currently at risk of collapse. CSIS has not supported the unit with resources commensurate with the importance of this unit in fulfilling CSIS's mission. The benefits of the AU are currently in jeopardy because of governance, human resource, and training deficiencies.

Finding no. 18: NSIRA finds that the AU's placement in the [Name] branch is not commensurate with its functions and importance. This governance anomaly most likely contributes to administrative hurdles and resource challenges faced by the AU.

Finding no. 19: NSIRA finds that without a functional AU able to produce timely and accurate warrant applications, CSIS puts at risk access to warrants and the information collected under them.

In view of these findings, NSIRA recommends that:

Recommendation no. 11: CSIS recognize the importance of the Affiant Unit by assigning affiants and analysts an employment classification congruent with their responsibilities.

Recommendation no. 12: CSIS create an Affiant Branch reporting directly to the CSIS Director.

Recommendation no. 13: CSIS urgently resource the Affiant Unit to meet its responsibilities and ensure its sustainability. In deciding the size of the AU, CSIS should assess how many warrants an affiant team might reasonably complete every year.

Recommendation no. 14: CSIS, in consultation with Justice, develop a comprehensive training course for all affiants and analysts, codifying best practices and methods for members of the AU.

Warrants counsel at NSLAG have several key roles in the warrant application process, and are intimately implicated in ensuring adherence to the duty of candour. Fostering a strong, collaborative, and productive relationship with CSIS is key. Morale among NSLAG warrants counsel may have suffered in light of the recent Federal Court decision that prompted this review. With recent staffing increases, it appears that NSLAG currently has the requisite complement to manage the number of annual warrant applications expected from CSIS, but recruitment challenges remain an ongoing issue. NSLAG should be staffed to ensure that CSIS's operations are not stalled due to the lack of availability of warrants counsel.

Recommendation no. 15: NSIRA recommends that NSLAG be staffed by a complement of counsel and support personnel sufficient to ensure that CSIS operations are not impeded by resource limitations at NSLAG.

The warrant application process is meant to be strengthened through a review of the near-final affidavit by an "independent counsel" (IC) – in practice, a lawyer drawn from the National Security Group (NSG) of the Department of Justice. The role was originally envisioned as performing a rigorous challenge of the warrant application. However, the primary role of the IC appears to be more clerical than substantive, designed to cite check rather than assertively perform a "devil's advocate" function.

NSIRA believes that the presence of a rigorous challenge function performed by a knowledgeable, adequately-supported lawyer distant from the warrant application is valuable and necessary. However, NSIRA proposes that the current IC model be abandoned in favour of a challenge function performed at Public Safety Canada, whose precise role is that of oversight of the CSIS warrant application process.

Working with the Public Safety unit charged with warrant review, an experienced and specialized warrant counsel could perform a genuine challenge role to the warrant, analogous to the role a defence lawyer would play were warrants subject to an adversarial process. NSIRA believes that a testing review of this sort will help forestall duty of candour shortcomings stemming from a failure to disclose fully information material to matters of potential concern about the broader context of the warrant and how it will be executed.

Finding no. 20: NSIRA finds that the "Independent Counsel" (IC) role as performed by NSG counsel falls short of creating a rigorous challenge function.

In view of this finding, NSIRA recommends that:

Recommendation no. 16: the function of the Independent Counsel as performed by NSG counsel at the Department of Justice be eliminated, in favour of a new challenge function, analogous to the role a defence lawyer would play were warrants subject to an adversarial process, situated at Public Safety and supported by the Public Safety vetting team, and performed by a knowledgeable lawyer from the Public Prosecution Service of Canada, the private sector, or elsewhere, who is independent from Justice management and not otherwise involved in CSIS warrant applications.

Once a judge issues a warrant, CSIS may execute the warrant. That execution must comply with the scope and terms of the warrant. However, the CSIS regional warrants coordinators have not

received sufficient training to enable the contents of warrants to be translated into advice on proper execution.

Finding no. 21: NSIRA finds that the CSIS regional warrants coordinators have not received sufficient training enabling them to translate the contents of the warrants into advice on proper warrant execution.

In view of this finding, NSIRA recommends that:

Recommendation no. 17: CSIS regional warrants coordinator positions receive adequate training, and that CSIS professionalize the position and enable warrant coordinators to more effectively translate the content of warrants into advice on warrant execution.

Investment in People

Concern about inadequate training at CSIS was a recurring theme in this review. This concern was noted in internal CSIS documents. CSIS acknowledges that it is currently not a learning organization and does not have a learning culture. There are too few training opportunities required to sustain a modern professional intelligence service operating in a complex environment.

Finding no. 22: NSIRA finds that CSIS lacks long-term training programs for Intelligence Officers.

Finding no. 23: NSIRA finds that CSIS has failed to provide systematic training programs for "non-Intelligence Officers".

Finding no. 24: NSIRA finds that the CSIS's Learning and Development Branch has not been sufficiently resourced to develop and administer comprehensive training programs, especially in specialized areas not covered by the training offered for Intelligence Officers early in their career.

In view of these findings, NSIRA recommends that:

Recommendation no. 18: CSIS adequately resource and regularly deliver evergreen scenario-based training programs for all CSIS employees, including;

- **annual, comprehensive, warrant training for all operational employees;**
- **specialized onboarding training for all employees not part of the Intelligence Officer program; and**
- **continued long-term training for all specialized personnel.**

Conclusions

This report concludes with observations on cross-cutting cultural and governance challenges that stem, at least in part, from challenges characterizing the provision of legal advice and the warrant process. NSIRA divides these broad, cross-cutting phenomena into two categories: morale and attitudes; and, performing the mission.

Low morale at CSIS was a common theme throughout this review. The systemic problems in the

warrant application process are likely one cause of this problem: morale is affected when a warrant acquisition system repeatedly prevents CSIS officers from performing their mandated duties, and is the source of regular reputational crises stemming from failures to meet the duty of candour.

Meanwhile, a failure to correct problems with the warrant process impairs CSIS and Justice's abilities to fulfill their mandates. Justice must go from being perceived as a roadblock, to a frank and forthright advisor fully attuned to operational objectives.

Within CSIS, the warrant application process was sometimes likened to winning a lottery – not because the Federal Court declines to issue warrants, but because of the resources required to prepare and complete the application. The current, laborious warrant application process is preventing some collection activities from moving forward.

In sum, this review was sparked by a compliance failure in a duty of candour matter. It concludes that repeated failures in this area are both caused by, and cause, deep-seated cultural and governance patterns. This vicious cycle has compounded the challenges of reform in the warrant acquisition process.

Cherry-picked or paper-based reforms that mask without addressing the overarching systemic, cultural, and governance challenges will suffer the fate of prior reforms: the problems will continue.

Finding no. 25: NSIRA finds that CSIS and Justice are at risk of not being able to fulfill their respective mandates. No one reform is likely to succeed unless each is pursued as part of a coherent package. No package will succeed unless backed by prioritization at senior levels, and the stable provision of resources, including people with the means and institutional knowledge to see reforms through, and no reform initiative will succeed unless accompanied by clear performance indicators, measured and analyzed regularly to track progress.

In view of NSIRA's findings above, and of prior unsuccessful reforms, NSIRA recommends that:

Recommendation no. 19: The recommendations within this review be treated as a coherent package and that progress and outcomes in implementing these recommendations be tracked, allowing management, the Ministers of Public Safety and of Justice, and NSIRA, to assess the efficacy of reforms and course-correct if necessary.

NSIRA intends to launch a follow-up review within two years that will measure progress at CSIS, Justice and Public Safety in resolving the systemic problem with the warrants process addressed by this review. Moreover, in other regular reviews implicating warrants, NSIRA will document recurrences of systemic problems. In the meantime, since this review originated with a decision of the Federal Court, it is vital that the Minister and CSIS share it in its full form with the designated judges of that court.

In recognition of the fact that this report was initiated following a recommendation of the Federal Court, NSIRA in turn recommends that:

(U) Recommendation no. 20: The full classified version of this report be shared with the designated judges of the Federal Court.

II AUTHORITIES

1. (U) This review was conducted under the authority of paragraphs 8(1)(a), (b) and (c) of the *NSIRA Act.*

III INTRODUCTION

2. (U) This review deals with how the Canadian Security Intelligence Service (CSIS) seeks and receives legal services from the Department of Justice (Justice) and obtains and executes warrants it needs to collect intelligence. In their current forms, these processes suffer from severe flaws due to systemic, governance and cultural issues. In this review, NSIRA found an intelligence service and its counsel who struggle to organize themselves in a manner that allows them to easily meet their legal obligations – towards the Federal Court in particular. NSIRA also found a failure to professionalize fully and sustainably the warrant process as a specialized trade that requires training, experience, and investment.

3. (U) This is not the first report on issues related to the warrant process. Since CSIS's creation in the 1980s, there have been several independent and internal reviews of various aspects of this topic, which are described in Annex A. Many of the findings made in this review echo those made in earlier assessments. In response to these reviews, CSIS has planned many reforms, initiated some, but persisted with only a subset. Though CSIS (and Justice) have made improvements, difficulties are still obvious. The failure to effect sustainable solutions following the multiplicity of reviews and duty of candour breaches is indicative of organizational struggles with deep rooted cultural issues that risk the execution of their mandates. With each incomplete reform, CSIS faces change fatigue that makes future course corrections more difficult. Yet the stakes are considerable.

4. (U) This report demonstrates the need to transform the relationship between CSIS and its legal counsel. It also points to the urgency of CSIS succeeding in fully professionalizing the warrant process, a prospect that appears to be in jeopardy. When implemented, the changes that are recommended will help to reestablish the Federal Court's trust in the warrant process. At the same time, legal support is not – and should not – be limited to the warrant process. As such, the review could not be restricted to the warrant process. It recommends reforms in the manner in which Justice gives legal advice to CSIS.

5. (U) The Federal Court's "judicial control" in overseeing the issuance of warrants is a key accountability safeguard in a country governed by the rule of law and attentive to rights and liberties. The warrants the Court issues, meanwhile, are the lifeblood of CSIS's functions as an intelligence agency – especially in an era where face to face interaction increasingly tends to be replaced by electronic communication.

6. (U) NSIRA heard repeated concerns from interviewees that the systemic problems rooted in governance and cultural issues risk creating an intelligence service incapable of meeting its intelligence mandate. These problems could also afflict other CSIS mandates potentially subject to judicial control, such as certain threat reduction measures. Urgently addressing challenges is therefore in the public interest. This review aims to recognize and encourage recent progress, while in some areas recommending new, essential reforms.

7. (U) This report first sets out the background to this review; the methodology NSIRA adopted for it; and the institutional and legal environment in which CSIS and Justice operate. The report then describes issues arising from Justice's provision of legal advice to CSIS and the manner in which CSIS and Justice construct a warrant application, ultimately presented to the Federal Court, and if granted, executed by CSIS. It also examines the question of training and skills-development, a recurring issue in this review. In each area, this report notes shortcomings,

while recommending reforms. The report ends with an examination of cross-cutting cultural and governance issues that are reflected in the warrant process, and which make change difficult.

8. (U) As the recommendations address the systemic, governance and cultural issues that are interrelated, a selective approach to their implementation will likely lead to the same outcome previous reviews have: repetition of the same problems, change fatigue and morale issues. The time has come for CSIS and Justice to face the harsh reality of potential failure to fulfill their mandates if they do not succeed with concrete governance, cultural and process change.

A. Review Background

9. (U) This review stemmed from a 2020 decision of the Federal Court (2020 FC 616). In that matter, the Federal Court recommended that a "comprehensive external review be initiated to fully identify systemic, governance and cultural shortcomings and failures that resulted in CSIS engaging in operational activity that it has conceded was illegal and the resultant breach of candour."[1] As a matter of law, before issuing such a warrant, the judge must believe on reasonable grounds that statutory pre-requisites are met and that the court should allow the invasive search. CSIS, assisted by Department of Justice lawyers, must fully apprise the judge of all information material to this decision.[2] Thus, the state must disclose to the judge, not just information supporting its application, but also information that weakens its case. The duty reflects the fact that a warrant proceeding is by necessity conducted in the absence of the proposed subject of the warrant, known as the "target", and closed to the public so the target is not alerted to the state's activities. The "duty of candour" in such proceedings aims to compensate for the absence of a party opposed to the state, by obliging the state to be especially frank and forthcoming about the merits of its application.

10. (U) At issue in 2020 FC 616 was whether CSIS should have told the Court about issues regarding the legality of CSIS human source activities that yielded information used in support of warrant applications. Some of these human source activities may have constituted terrorism offences in Canadian law. This was not the first instance of duty of candour problems – indeed, such problems have been a recurring feature of CSIS's warrant practice.[3] Because CSIS has repeatedly struggled with the duty of candour in its warrant applications, the Federal Court in 2020 FC 616 recommended an external review of both Justice and CSIS.

11. (U) In response, on June 23, 2020, the Minister of Justice and the Minister of Public Safety and Emergency Preparedness jointly referred the matter to NSIRA under paragraph 8(1)(c) of the *NSIRA Act*. NSIRA also chose to exercise its own independent jurisdiction under paragraph 8(1)(a)(b) to initiate this review.

---

1 2020 FC 616, Pg. 124, Para 2 (The Court's Judgment).

2 This report does not purport to convey a full overview of the duty of candour. It does, however, describe this duty at various points. For example, please refer to paragraph 117 for a more detailed discussion of materiality in the CSIS warrant context. For this introduction, NSIRA simply points to the discussion in 2021 FCA 92, the Federal Court of Appeal decision stemming from the crown immunity matter that sparked this review. There, the Court observed that material information is all information "relevant to the determination that a judge must make in deciding whether or not to issue a warrant, and if so on what terms." This includes facts that "would tend to go against what is sought". And it includes identifying "the legal issues raised by an application" (at paras 127 and 129). That means that the affidavit supporting the warrant application must be "full and frank" and "clear and concise" in its disclosure of all these material facts. It should "never attempt to trick its readers" and should resist the "temptation of misleading the authorizing judge, either by the language used or strategic omissions" (at para 128, citing *R v Araujo*, 2000 SCC 65 at para 46-47),

3 Please see *Annex A*

12. (U) While the Federal Court of Appeal subsequently allowed the government's appeal of the decision in 2020 FC 616, its holdings did not disturb – and indeed, reaffirmed -- the lower court's core preoccupation with the duty of candour.[4]

B. Methodology

13. (U) NSIRA conducted this review during a pandemic that frequently impaired access to its facilities housing classified information. This reality presented challenges and inevitable delays for both NSIRA and the reviewed departments.

14. (U) NSIRA made this a "Member-led review". Specifically, one or both of the two assigned NSIRA members (Marie Deschamps and Craig Forcese) managed the review process, reviewed the documents, participated in most of the CSIS and Justice briefings (and reviewed the transcripts of others), conducted most of the confidential interviews, and led the writing of this report. A specialized team at NSIRA participated in every aspect of the work.

15. (U) NSIRA drafted broad Terms of Reference to govern this review, with a heavy focus on the CSIS warrant application process and the manner by which Justice conveys legal advice to CSIS. As the review evolved, it became clear that the problems with the CSIS warrant process are more properly a symptom of broader systemic, governance and cultural issues at both CSIS and Justice, including Justice's specialized legal services unit supporting CSIS, the National Security Litigation and Advisory Group (NSLAG). NSIRA therefore examined not only the operational provision of legal advice and the warrant process, but also information management, the use of technology, and related training programs. While the Terms of Reference indicate that the review covers the period of January 1, 2015 to September 30, 2020, NSIRA took into consideration information outside this period in order to fully understand the issues at play.

16. (U) This report does not revisit the specific circumstances of 2020 FC 616, nor does it conduct a forensic accounting of the events leading to it. From time to time, the report makes observations related to that case in order to contextualize findings. However, this review was intentionally forward-looking, reflecting the fact that CSIS and Justice have introduced (or proposed) reforms since the 2020 decision.

17. (U) In conducting this review, NSIRA relied on both its regular process and confidential interviews. Under its regular protocols, it issued a number of requests for information, reviewed the documents provided, and received briefings from CSIS and Justice. In the case of CSIS, NSIRA also used its direct access to CSIS systems to retrieve information independently. Among other things, NSIRA examined the complete record of a recently filed complex warrant application.[5] Most briefings involved CSIS and Justice managers describing their policies, governance structures, and practices. NSIRA heard about a number of initiatives – some that are planned, others underway or partially implemented, and still others abandoned.

---

[4] On May 12, 2021, the Federal Court of Appeal (FCA) issued its judgement in the appeal of the earlier Federal Court decision. The decision reiterated the importance of the duty of candour but found that the Federal Court had erred in holding that the duty of candour required the Service to proactively seek waiver of solicitor-client privilege and disclose legal advice in a warrant application. The decision was specific to one of the three warrant applications addressed in the underlying decision, in regards to "the treatment of the duty of candour issue as it related to the legality of [redacted] and the Service's reliance on information obtained [redacted] 2021 FCA 92 at para 88. The decision does not overturn the court's initial recommendation regarding the institutional, systemic governance and cultural issues.

[5] NSIRA examined a [redacted] warrant application filed in 2020 [redacted]. NSIRA examined the file in detail and briefed with the affiants and Counsel who presented this application before the FC.

18. (U) To supplement these briefings, NSIRA adopted an innovative approach to this review by also conducting dozens of confidential interviews with former and current management and staff at all levels from CSIS and Justice. These interviews were conducted in the absence of CSIS or Justice supervisors and without their knowledge. NSIRA conducted these interviews under a strict guarantee that it would protect the identities of those who participated. At the outset, the NSIRA Members leading the review met with both the Director of CSIS and the Deputy Minister of Justice. Following the meeting, both officials encouraged members of their management and staff to participate in confidential, in-person interviews with NSIRA. NSIRA thanks both leaders for their explicit support, including through their internal communications with their employees. NSIRA especially thanks all the individual employees who then participated in these confidential interviews and trusted NSIRA's promise of anonymity.

19. (U) In some instances, NSIRA selected individuals to ensure it had full coverage of the warrant process and invited them to participate in a confidential interview. Other interviewees contacted NSIRA and offered to participate. Some interviewees occupied operational positions at CSIS, while others worked on legal and policy matters. Some interviewees had daily exposure to the warrant process, while others had had more episodic exposure to the process. Since NSIRA conducted these interviews with the understanding it would protect the identities of interviewees, NSIRA has drafted this report carefully to honour this undertaking and has not identified interviewees by name or by position revealing their identity.

20. (U) The individuals who participated in confidential interviews with NSIRA were frank, professional, insightful about their experiences, and open. Interviewees did not come to voice personal grievances, nor were they inclined to defend past practices as ideal. Rather, the interviewees displayed a genuine commitment to their organizations' mandates and a sincere desire to see positive, lasting change. Where they expressed dissatisfaction, it stemmed from earnestly (and often deeply held) concerns that their organization was falling short of meeting its mandate, and that the warrant process reflected certain organizational shortcomings. These interviews were essential for "ground-truthing" the knowledge NSIRA had gained from documents and formal briefings. They also raised issues and perspectives that would otherwise have been unavailable to NSIRA.

21. (U) NSIRA also consulted external experts on national security, organizational development, and human resources. These conversations contributed to NSIRA's understanding of the systemic, governance, and cultural issues that often develop in organizations. NSIRA conducted a small number of discussions with foreign counterparts who have dealt with similar issues in the past. In addition, NSIRA consulted with experts who had been, in the past, involved in reviewing similar issues relating to CSIS. NSIRA is grateful to these experts for their generosity in contributing to this review. All of NSIRA's discussions with stakeholders external to the Canadian government took place at the unclassified level.

22. (U) Finally, as part of its standard protocol, NSIRA presented the draft report to both CSIS and Justice for factual accuracy verification. This part of the process provides reviewees with the opportunity to signal factual omissions or errors, if any. At the end of the factual accuracy verification period, the members met with the Deputy Minister of Public Safety and again with the Director of CSIS and the Deputy Minister of Justice. NSIRA thanks them for their time and openness.

23. When examining the insights of its interviewees and throughout the finalization of this report, NSIRA was alive to the particular challenge of disaggregating legacy issues from contemporary concerns. During briefings and in comments received on the draft report, the departments noted projects, initiatives and reforms either being planned, scheduled for execution, or underway. NSIRA acknowledges the initiatives upon which it was briefed. However, this report

focused on ascertaining the existing challenges with the provision of legal advice and the warrants process. NSIRA did not discount existing issues and challenges simply on account of promised (but not yet fully achieved) administrative reforms. NSIRA is confident that the issues described in this report persist as of the second half of 2021. As described at the end of this report, NSIRA intends to undertake a further review in two years' time to assess progress in implementing the report's recommendations. At that time, NSIRA will have an opportunity to assess whether any reform initiatives have been successful.

24. (U) Confidence Caveat: Some of the documents provided by the reviewed institutions have not been independently verified by NSIRA. However, to a large extent, NSIRA was able to verify much of the information relied upon in this review through NSIRA's own confidential interviews. In addition to this direct access to staff, NSIRA was able to use its direct access to CSIS information repositories to confirm information that it needed to verify and to pursue necessary additional inquiries. For that reason, NSIRA has a high level of confidence in the information on which it relied to complete this review.

C. Institutional Environment

1. Systemic, Governance and Cultural Issues

25. (U) In this review, NSIRA makes recommendations on systemic, governance, and cultural issues that contribute to inefficiencies and may threaten the ability of CSIS and Justice to fulfil their mandates.

26. (U) NSIRA defines "systemic" issues as ones affecting an organization as a whole, in the sense that they are not the consequence of a specific individual or isolated factor. "Governance" refers to the rules, practices and processes by which managers direct and control an organization. Governance addresses three key questions: how are decisions made; who makes the decisions; and who is accountable.[6] Organizational "culture" is the way in which, over time, the members of an organization learn to work in a particular setting by developing a set of shared understandings. These understandings may be based not only on formal policies but also on assumptions and practices that members develop in response to the implicit rules and influences governing their organization.

27. (U) These three concepts operate together and are interconnected. For example, inadequate governance may be the source of deficiencies in training programs that may prompt increased requests for legal support, which in turn create resource management issues, delays in providing advice, and operational hurdles. These operational challenges may give rise to systemic issues, while imperfect workarounds to these problems may eventually become embedded as cultural practices.

28. (U) Systemic issues tied to governance and cultural issues may impede CSIS and Justice from fulfilling their mandates, while also meeting their obligation to adhere to the rule of law. In this last respect, Canada is a "rule of law" country. Among other things, the "rule of law" means that the state is subject to, and not above, the law. It only has the powers conferred upon it by law, and any exercise of state power must be traced to a law. Indeed, as discussed next, both CSIS and Justice operate in a highly legalized environment.

29. (U) The next section will briefly describe the basic legislative and operational framework of both CSIS and Justice.

---

6 See: https://iog.ca/what-is-governance/, and https://.un.org/milleniumgoals/pdf/Think%20Pieces/7_governance.pdf

2. Legal and Operational Structures

a. CSIS

30. (U) The *CSIS Act* is the statute of Parliament that created CSIS, and confers upon CSIS certain powers to discharge its mandates. The key mandates implicated in this review are security intelligence (or "section 12 investigations") and foreign intelligence (or "section 16 investigations"). Both of these types of investigations have their own distinct pre-requisites – not least, the conditions that CSIS must meet before it undertakes an investigation and then applies for a warrant under section 21.

31. (U) CSIS is one of several security organizations found within the portfolio of the Minister of Public Safety and Emergency Preparedness (Minister of Public Safety). CSIS is accountable to this minister, and this minister is in turn responsible to Parliament for CSIS.

32. (U) The manner in which CSIS discharges its mandates is governed by the *CSIS Act* and Ministerial Directions issued by the Minister of Public Safety. For instance, in 2015 and 2019, the Minister issued Ministerial Directions addressing issues of accountability. The 2015 Ministerial Direction (2015 MD) for Operations and Accountability[7] states the fundamental principles that guide all of CSIS's operations. The 2015 MD is premised on the expectation that *"the service will perform its duties and functions with due regard for the rule of law…"*[8]

33. (U) Other laws are pertinent to CSIS. Especially relevant for this review are Part VI of the *Criminal Code of Canada*, which governs the interception of private communications, and section 8 of the *Canadian Charter of Rights and Freedoms*, which protects the reasonable expectation of privacy against state searches and seizures. CSIS must acquire judicial warrants from the Federal Court before it embarks on investigative techniques that would otherwise violate these laws.

34. (U) Under the *CSIS Act*, CSIS is led by a Director who holds the status of deputy head of the organization. The Director performs the leadership function assisted by a team of executives responsible for specific business lines within CSIS, including the Deputy Director Operations (DDO). The DDO is responsible for CSIS's operations across all active investigations.[9] The CSIS management structure also includes an Assistant Director Legal (ADL), a position occupied by the NSLAG' Executive Director (discussed below).

35. (U) CSIS converts legal requirements into administrative processes through policies. Critically, it has struggled to do so. The CSIS operational policy suite has been incomplete and out-of-date for a number of years, a finding noted repeatedly by both NSIRA's predecessor, SIRC, and by NSIRA.[10] This issue was again pervasive in the course of this review, making it difficult to precisely describe the formal operational policy environment applicable to the warrant acquisition process throughout the period covered by this review. The consequences of this shortcoming are considerable. Policies are the building blocks of any organization. They guide

---

7 *Ministerial Direction for Operations and Accountability*, Minister of Public Safety and Emergency Preparedness, 31 July 2015.

8 Ibid.

9 Reporting to the DDO are the Assistant Director Collection (ADC), the Assistant Director Requirements (ADR) and the DG of Human Sources and Operations Security (HSOS). The ADC manages and overseas all domestic and foreign collection activity, this includes collection in six regional offices (as well as International Region). The ADR is responsible for the managements and oversight of CSIS's national operations and intelligence requirements, intelligence analysis and dissemination activities, and security screening program. The Affiant Unit and [Name] units report to the [Name]

10 NSIRA 2019 Annual Report at para 29-31.

the conduct of its members from the bottom up to the senior leadership. Without clear policies, employees are likely to devise their own interpretations of how to act and of the limits of their powers, causing confusion and making legal compliance difficult.

b. Justice and NSLAG

36. (U) The Department of Justice provides legal services to departments and agencies on a broad range of issues across the federal government.[11] Its mandate is to support the dual roles of the Minister of Justice and the Attorney General of Canada (AG).[12]

37. (U) The Minister of Justice, as the official legal advisor to Cabinet, is responsible for the general management and direction of the department, and for ensuring that the administration of public affairs is in accordance with the law. The Minister is responsible for matters related to the federal administration of justice. The Minister exercises political judgment, except when providing legal advice, which must be independent and non-partisan.[13]

38. (U) The Minister is also *ex officio* the AG, also referred to as the Chief Law Officer of Canada. The role of the AG is to provide legal advice and legislative services to government departments and agencies, and to conduct litigation on behalf of the government.[14] Importantly, the AG represents the Crown and not individual departments or agencies, and therefore seeks to protect whole-of-government interests. Although departments generally act as the instructing clients, it is the Attorney General's responsibility to facilitate, with these departments, adherence to the rule of law.

39. (U) The Deputy Minister (DM) of Justice, who is also the Deputy Attorney General of Canada, manages the work and operations of the department as its most senior public servant. The DM is supported by an Associate Deputy Minister who is entrusted to lead some of Justice's specialized portfolios.[15] This includes the Public Safety, Defence and Immigration (PSDI) Portfolio which is led by an Assistant Deputy Minister reporting directly to the Associate Deputy Minister.[16]

40. (U) Justice delivers legal services to federal departments and agencies through a mix of three models, all of which apply to CSIS: (1) specialized centers of expertise, within the department;[17] (2) a network of regional offices located across the country; and (3) dedicated legal service units (LSUs) that are physically located with the departments they advise.

---

11 The *Department of Justice Act*, creates the Department of Justice, over which the Minister of Justice presides, and sets out the powers, duties and functions of the Minister of Justice and Attorney General of Canada.

12 These are two separate positions held by one person.

13 Department of Justice, "Roles and Responsibilities of the Minister of Justice and the Attorney General of Canada", *Department of Justice Canada Minister's Transition Book*, See also *Department of Justice Act*, section 4. See also Department of Justice, "Roles and Responsibilities of the Minister of Justice and Attorney General of Canada", Department of Justice Canada Minister's Transition Book, Book of Documents [Protected B] (October 9, 2020), Tab 3.

14 Note that the Department of Justice does not conduct criminal prosecutions, which forms part of the role of the Attorney General of Canada. Rather, that responsibility lies with the Public Prosecution Service of Canada whose main objective is to prosecute federal offences. It also provides legal advice and assistance to law enforcement.
Department of Justice, "Roles and Responsibilities of the Minister of Justice and Attorney General of Canada", Department of Justice Canada Minister's Transition Book, Book of Documents [Protected B] (October 9, 2020), Tab 3

15 Department of Justice, [Org. Chart], Book of Documents (October 9, 2020) [Protected B], Tab 4.

16 F. Daigle, Briefing Transcript (October 9, 2020) [Protected B], p. 9, lines 23-24.

17 Specialized branches include constitutional, human rights, and access to information and privacy law matters. Specialized branches ensure that all departments and regions take a consistent, "government-wide" approach to the law in these areas. [redacted] Department of Justice [redacted] "The Role of the Department of Justice | Le rôle du ministère de la Justice", Book of Documents (October 9, 2020) [Top Secret], Tab 10 4th page.

41. (U) LSU counsel provide day-to-day advice on all issues. LSU counsel may consult or collaborate with counsel from the specialized branches, or at other LSUs as needed.[18] Although co-located with client departments, LSU counsel are Justice employees, and in keeping with the status of the Attorney General, must remain independent from the client.

42. (U) The National Security Litigation and Advisory Group (NSLAG) is the LSU that supports and advises CSIS. It is located at CSIS headquarters and is part of the PSDI Portfolio. With approximately 50 counsel positions,[19] NSLAG is led by an Executive Director and Senior General Counsel who reports directly to the Assistant DM of PSDI.[20] The two meet every two weeks to discuss NSLAG's work. The ADM, in turn, must report any matters of concern to the Associate DM.[21]

43. (U) As mentioned previously, NSLAG's Executive Director also occupies the position of ADL within the CSIS executive structure, reporting to the Director. Justice described this reporting relationship as functional only.[22] In the ADL role, the head of NSLAG has confidential, bilateral meetings with the CSIS Director, to provide briefings on legal files and discuss issues that arise.[23] This functional reporting relationship to the client co-exists with the formal reporting relationship within Justice. While at first glance this functional reporting role might seem to pose a challenge in terms of maintaining full independence from the client, Justice asserts that this structure is not unique to CSIS and does not create concerns regarding client capture.[24]

44. (U) NSLAG provides both advisory and litigation services to CSIS on its security and intelligence operations. Its advisory work involves matters related to the duties and functions of CSIS, including questions of legal authority, and advice related to the *Charter*, threat reduction measures, and the application of other legislation to CSIS operations. NSLAG's litigation work consists mainly of representing CSIS in applications for warrants before the Federal Court and related matters, and representing both CSIS and other government departments and agencies in complaints investigations before NSIRA.[25]

45. (U) CSIS also receives legal services from the National Security Group (NSG), a specialized legal branch located at Justice's headquarters. As part of the AG's National Litigation Sector, NSG leads the litigation of claims related to national security privilege under section 38 of the *Canada Evidence Act*. Its counsel are security cleared at the Top Secret level.[26] NSG counsel also play a role in the CSIS warrant application process – namely, to conduct an "independent challenge" exercise as part of the internal approval process for warrant applications. NSG's role

---

18 [redacted] Department of Justice [redacted] "The Role of the Department of Justice Book of Documents (October 9, 2020) [Top Secret], Tab 10 [pages 3-4]. L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 14, lines 5-10.

19 Department of Justice, NSLAG Consolidated Legal Services Organizational Chart. October 9, 2020, Book of Documents, Tab 4.
While the Organizational Chart includes over 50 counsel positions, almost one-third were unfunded at the time of writing.

20 Department of Justice, "NSLAG Roles and Responsibilities", Book of Documents (October 9, 2020) [Top Secret], Tab 5, p.1; L. Johnson, Briefing Transcript (October 9, 2020) (TS), p. 10, lines 22-24.

21 L. Johnson, Briefing Transcript (Oct 9, 2020) [TS], p. 11, F. Daigle, Briefing Transcript (Oct 9, 2020) [Prot B], p. 9.

22 Department of Justice, Canadian Security Intelligence Service / [Organizational Chart], Book of Documents [Top Secret], Tab 2. L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 11, lines 12-14.

23 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 17, lines 12-14.

24 The same model exists for all LSUs throughout Justice, with LSU heads participating as members of their client department's executive committees. Justice informed NSIRA that client departments understand this relationship well. In particular, client departments understand that the role of the LSU heads on their executive committees is as a representative of Justice, to provide legal services. F. Daigle, Briefing Transcript (October 9, 2020) [Top Secret], p. 13, lines 7-14. See also L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 14, lines 5-16; CSIS Legal Services Unit (Department of Justice and CSIS), "Assistant Director Legal", Book of Documents (October 9, 2020) [Top Secret], Tab 3.

25 Department of Justice, Book of Documents (October 9, 2020) [Top Secret], Tab 1, p. 1. See also Department of Justice, "NSLAG Roles and Responsibilities", Book of Documents (October 9, 2020) [Top Secret], Tab 5, p. 2.

26 F. Daigle, Briefing Transcript (October 9, 2020), p. 26, lines 7-10

as Independent Counsel (IC) in the CSIS warrant application process is discussed in section 4 e. below.

46. (U) While the basic legislative and operational framework may seem simple, a closer analysis sheds light on many ongoing issues.

IV ANALYSIS

47. (U) This review revealed governance and cultural challenges in both CSIS and Justice that contribute to systemic issues in the warrant process, including with respect to the duty of candour. NSIRA's findings fall within three overarching areas:

A. Justice's provision of legal advice;
B. CSIS and Justice's management of the warrant acquisition process; and
C. Investment in people in terms of training.

The report concludes with comments on systemic, governance and cultural issues.

A. Justice's Provision of Legal Advice

48. (U) In order to meet its obligations with regard to the rule of law, CSIS must know what the law is. An unwieldy, tardy or indefinite means of ascertaining the lawfulness of activities jeopardizes CSIS's ability to fulfill its mandate while adhering to the rule of law. This review considered, therefore, the fashion in which Justice (and specifically, NSLAG) provides legal advice to CSIS in performing its mandated activities, and how it has organized itself to do so. NSIRA noted three specific issues: the bureaucratic manner of obtaining advice; its timeliness; and the usefulness of this advice to CSIS in meeting its mandate.

1. Giving Advice to CSIS

49. (U) CSIS operates in often rapidly evolving and legally challenging environments. Timely, nimble and actionable legal advice is critical. To meet these objectives, Justice has adopted "operating principles", including a centralized "one-voice" model for delivering legal services. In this model, Justice counsel are described as speaking "with one voice",[27] reflecting a desire for uniform and consistent legal advice delivered on behalf of the AG. To this end, Justice seeks consistency in the legal advice provided and the legal positions taken across Justice, to ensure a "whole-of-government" approach.[28] Its advice does not simply reflect the opinion of the assigned legal counsel. Rather, the advice provided has "all of Justice behind [it]".[29]

50. (U) The one voice approach responds to a prior era in which many federal government departments hired their own lawyers to provide them with legal advice. These lawyers were not part of Justice. When difficult, cross-governmental legal issues arose, counsel representing the various ministries did not always agree, which would then place the AG in a difficult position in Cabinet.[30] A decision was made to bring all such departmental lawyers together in a common legal service operating under the Justice umbrella.

---

27 F. Daigle. Briefing Transcript (October 9, 2020) [Protected B], p.14, line 6 – p. 15, line 3; L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 19, lines 9-16.

28 F. Daigle, Briefing Transcript (October 9, 2020) [Protected B], p.15, lines 4-11.

29 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 14, lines 11-15; L. Johnson, Briefing Transcript (October 9, 2020) [Protected B], p. 38, lines 21-23.

30 F. Daigle, Briefing Transcript (October 9, 2020) [Protected B], p. 14, lines 8-18, citing the Glasgow Report.

51. (U) In support of its one voice approach, Justice now employs a number of tools, including:

- establishing centers of expertise within Justice to provide consistent, "government-wide" advice, primarily to Legal Services Units, in key areas of public law, such as constitutional law, human rights law, and information and privacy law;[31]
- maintaining a legal knowledge portal called "Justipedia" to serve as a single, national, searchable repository for all legal opinions from Justice's services;[32]
- fostering discussion of legal issues at various committees, such as the national and regional litigation committees and other *ad hoc* committees;[33]
- convening working groups to determine legal positions;[34]
- creating practice groups to exchange and share relevant knowledge; and,
- applying a common legal risk management (LRM) framework when providing advice to client departments and agencies.[35]

52. (U) While the premise for the one voice approach is sound, this review has noted some disadvantages in the current implementation of the model in the CSIS context. Importantly, because of the bureaucratic process required to complete a legal opinion, obtaining legal advice can be burdensome, inefficient, and a source of undue delay. Hierarchies in both CSIS and Justice have impeded fluid collaboration between Justice counsel and their CSIS client by limiting counsel's ability to deliver advice rapidly. The pace of legal advice-receiving from Justice is slower than a CSIS intelligence operation, which leads to the advice not being delivered in a timely manner and in CSIS being [discussion of how collection activities are affected][36]

53. (U) In addition to the challenges of timeliness associated with bureaucratic hierarchies, there are also communication challenges associated with the different knowledge base involved in legal analysis versus operational expertise. NSIRA noted several critiques. Interviewees urged that Justice counsel would benefit from a greater understanding of CSIS's operations. It was suggested that new or junior lawyers could participate in key operational training sessions to gain a better understanding of the CSIS context. Some discussed current initiatives to cultivate greater understanding between Justice and CSIS, voicing skepticism about their success. For instance, Justice was said to pitch its "lunch and learn" sessions with CSIS at the wrong level, and is too esoteric and theoretical when discussing, for example, section 8 of the *Charter*.[37] Legal training of CSIS employees conducted by inexperienced counsel was also identified as a problem.[38]

54. ~~(S/C)~~ These complaints are consistent with a 2018 client feedback survey on CSIS legal advisory services. That survey measured four dimensions of its service in comparison to those

---

31 Additional centres of expertise include: administrative law, labour law, business and technology law, procurement law, official languages, and legal services supporting the Privy Council Office. See F. Daigle, p. 11, line 23 – p. 12, line 8; F. Daigle, Briefing Transcript (October 9, 2020) [Top Secret], p. 22, line 21 – p. 23, line 11; [redacted] Department of Justice [redacted] "The Role of the Department of Justice, Book of Documents (October 9, 2020) [Top Secret], Tab 10 [4th page]

32 PSDI Portfolio Evaluation, p. 28 of 37; F. Daigle, Briefing Transcript (October 9, 2020) [Top Secret], p. 23, lines 12-16. Additionally, NSLAG maintains its own classified SharePoint site for its Top Secret material called "Justipedia Classified". Ref. DoJ Factual Accuracy Check, December 21, 2021. L. Johnson, Briefing October 9, 2020.

33 F. Daigle, Briefing Transcript (October 9, 2020) [Protected B], p.19-20.

34 L. Johnson, Briefing Transcript (October 9, 2020) [Protected B], p. 38, lines 8-11, and p. 56, line 24- p. 57, line 5.

35 A. Saranchuk, Briefing Transcript (October 9, 2020) [Protected B], p. 68.

36 Interview(s).

37 Interview(s).

38 Interview(s).

of the overall PSDI Portfolio.[39] The survey found the overall quality of legal advisory services fell slightly below the departmental target, landing in the "moderate" category, with similar ratings from CSIS on the overall accessibility and responsiveness, as well as usefulness of its legal services. The survey results demonstrated satisfaction with legal risk management, which met the target standard.[40] On the issue of timeliness, however, Justice scored poorly. Justice concluded that the survey indicated that CSIS users were, by and large, somewhat unsatisfied with the services provided and that there was room for improvement. Some comments from CSIS consistent with those frequently echoed in the interviews conducted by NSIRA included:

- *"I don't get the impression that DOJ lawyers working within my organization actually comprehend what we do."*
- *"Responses take too long. Has impact on our operational abilities.* [discussion of how collection activities are affected] *"*
- *"Justice staff were adept at pointing out…legal risks associated with initiatives, but were not adept at providing practical advice to mitigate risk (other than recommending cessation of the initiative)"*
- *"There seems to be a lack of coordination."*[41]

55. (U) The following sections describe more detailed and pointed CSIS preoccupations with the manner by which its officials seek advice from Justice and about the nature of the resulting advice.

a. Obtaining Advice

56. (U) Barriers to accessing legal advice were a common theme of interviews. CSIS must formally frame its questions as clearly as possible, to avoid "half-baked" inquiries.[42] However, rather than a collaborative process between counsel and CSIS, the conventional advice-seeking system is a formalized, bureaucratic process. Formal advice requests generally appear to be funneled from CSIS investigators and related personnel in the regional offices through their hierarchies, sometimes (but not usually) up to headquarters, and then from there to Justice counsel.

57. (U) This process, and resource constraints at Justice, contribute to considerable delays, [description of timeline] [43] Apart from prioritized, urgent requests for legal advice, it can take [timeline] to receive legal advice. In situations involving novel or complex issues, advice may take [timeline] [44]

58. (U) Once prepared, advice then filters back through the same hierarchy, sometimes never

---

39 The four overall dimensions of service were: Accessibility/Responsiveness of Legal Services; Usefulness of Legal Services; Timeliness of Legal Services; and Legal Risk Management. Department of Justice, Book of Documents [Top Secret], (October 9, 2020), Tab 12, p. 6.

40 The survey results focused on Legal Advisory Services only, since there was an insufficient number of users for Litigation, Legislative Drafting and Regulatory Drafting Services. The survey was administered in 2018. The previous survey of CSIS was in 2011. Book of Documents [Top Secret], (October 9, 2020), Tab 12, pp. 3, 5, 9 and 10.

41 Department of Justice Canada, Legal Services Client Feedback Survey: Comments from the Canadian Security Intelligence Service Client Organization. March 2019. Briefing book October 9, 2020, Tab 13, pp. 1-2.

42 Interview(s).

43 Interview(s), NSIRA, DoJ Advisory Briefing (D. Robinson) March 16, 2021.

44 Interview(s).

reaching the investigators in its full form. Some interviewees reported concerns about "broken telephones" in which advice requests morphed in their travels through the hierarchy without an iterative process between counsel and the investigators seeking the advice, resulting in legal advice of limited relevance.[45]

59. (U) Since this conventional process implicates both CSIS and Justice, it can be difficult to ascertain how much of this reported delay stems from Justice's advice-giving mechanics and how much from CSIS's own internal bureaucracy. Moreover, statements by interviewees estimating delay in receiving advice are hard to corroborate since NSLAG does not track the time it takes to provide its advice.[46] The absence of such data at Justice raises a separate issue of whether it is in a position to measure progress and improvements stemming from any reform initiative.

60. (U) Regardless of precise cause, the lack of clear timely advice has reportedly had considerable impact on CSIS operations. With an increase in electronic communication and information, the need for timely, clear advice on investigative methods has become pivotal.[47] The operational impact is notable: interviewees repeatedly described an [discussion of detrimental effects on operations] that may require legal advice. Managers have reportedly sometimes advised staff to seek alternative solutions where a matter may require legal advice [redacted] [discussion of detrimental effects on operations][48]

61. (U) Clearly, the conventional legal advice process does not adequately support CSIS operations, both in terms of timeliness and relevance.

b. The Nature of the Legal Advice

62. (U) In addition to timeliness and relevance, NSIRA heard regular and often related concerns about the nature of the legal advice supplied by NSLAG to CSIS. NSIRA interviewees repeatedly described legal opinions pitched at an esoteric and legalistic level, without sufficient attention to the audience that needs to understand and act on them.[49]

63. (U) NSLAG has typically presented its advice as a legal risk assessment, in which NSLAG opines on the risk associated with a specific activity, in accordance with the Justice Legal Risk Management (LRM) Framework, described further below. The style of the resulting advice can be compared to a "traffic light" system, where an activity represents a low legal risk to CSIS (green light); a high legal risk (red light); or, more ambiguously, an intermediate legal risk (yellow light). Yellow light-style responses were reportedly the most common and the most frustrating to consumers of the advice, especially when unaccompanied with discussions of how risk could be mitigated.[50]

---

45 Interview(s).

46 NSIRA, DoJ Information Management Briefing, July 20, 2021. Pgs. 26-29.
NSIRA, DoJ Advisory Briefing (D. Robinson) March 16, 2021.
NSIRA heard differing narratives regarding the ability and ease of collecting business analytics such as the average time to provide legal advice to CSIS. DoJ management noted that the business data is available to be mined and is organized and presented from time to time. This did not align with the information provided by the IM expert who noted that business analytics are difficult to gather en masse and may necessitate looking at the individual file metadata in order to gather information.

47 Discussed further under warrants, survey results. Interview(s).

48 Interview(s).

49 Interview(s).

50 Interview(s).

64. (U) In this last respect, CSIS interviewees often described NSLAG opinions as not making efforts to propose alternative and legally sustainable means of arriving at the intended objective. That is, NSLAG reportedly does not always understand CSIS's objectives, and then provide advice designed to guide CSIS on how it might lawfully meet that objective (if possible). Several CSIS interviewees emphasized the potential value of having Justice assist them by providing advice in the form of a "road map" to how an operation might reach its objective lawfully. They stressed, however, that this road map-style form of advice was not a regular part of the NSLAG advice-giving approach or practice culture.[51] That said, NSIRA also heard that there may now be the beginnings of a shift from the conventional advice-giving approach, as discussed below.[52] Because of the importance NSIRA places on it, this report returns repeatedly to the concept of road map-style advice.

65. ~~(S)~~ NSIRA heard that in instances where CSIS managers received advice indicating a medium level of risk (yellow light), they often [description within CSIS of an unwillingness to accept risk] [redacted][53] In other instances, managers expressed discomfort with assuming the risk and reportedly forwarded the decision up the hierarchy to diffuse responsibility.[54] Operationally, such delays in decision-making often have detrimental effects on investigations.

66. (U) As a result, some at CSIS perceive Justice as presenting a road-block.[55] This is not because Justice provides principled and clear positions reflecting the primacy of the rule of law over ill-advised operations, but rather as a result of the bureaucracy at Justice, its perceived operational illiteracy, and its unhelpful approach to communicating legal advice.

67. (U) There is, however, another dimension to these issues. Justice, and NSLAG especially, face challenges in giving advice to CSIS. Justice is not directly analogous to a private sector law firm. It must perform a public law function tied to the roles of the Minister of Justice and the AG. In giving its legal advice, Justice must be especially attentive to the rule of law and the AG's role in defending it.

68. (U) When interacting with its clients, Justice acts merely as an advisor and sees it as its client's responsibility to make the ultimate decision, informed by the advice given. A factor that may explain Justice's resistance to go beyond pure legal analysis is that Justice is necessarily wary of a reported tendency by CSIS to recast legal questions in an effort to get different answers.[56] CSIS, it was said, sometimes resists the law as it is, hoping that the law will be what it wants it to be.[57]

69. (U) Additionally, NSIRA heard that CSIS has not always shared all relevant information with Justice, prompting a degree of mistrust.[58] NSIRA heard of instances in which CSIS provided Justice with partial information, but did not convey the full picture.[59] NSLAG has informed CSIS that to provide the most meaningful legal advice and to better support its operations, counsel need to have "all the facts", and to be engaged "sooner and deeper".[60] NSLAG conveyed that earlier and ongoing involvement throughout the stages of an investigation or operation, with

---

51 Interview(s).
52 Interview(s).
DoJ (K Unger) Briefing Transcript (December 18, 2020) [Top Secret], pgs. 16-17.
53 Interview(s).
54 Interview(s).
55 Interview(s).
56 Interview(s).
57 Interview(s).
58 Interview(s).
59 Interview(s).
60 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret] pgs. 16-17, and 68. L. Johnson, Briefing Transcript (July 15, 2021) [Top Secret] p. 43, lines 5-9.

participation in CSIS meetings and discussions along the way, would enable counsel to gather facts more naturally, and permit a more nuanced understanding. If there is uncertainty as to the client's true goals and current situation, it is understandable that Justice lawyers are sometimes reluctant to provide a road map.

70. (U) The provision of advice on highly classified matters also presents logistical challenges. NSLAG lawyers operate in an environment that may impede easy interaction with other components of Justice, including in the specialized practice groups, where top secret security clearance holders are few and information management systems are not approved for classified information storage. Further, Justice is not well structured to address the range of matters arising in national security,[61] and other units may produce advice that is too late, or unhelpful.[62] Specialized units struggle where they are excluded from relevant classified information, and have sometimes been consulted by NSLAG too late in the advice process.[63] The process by which differences of opinion between these specialized groups and NSLAG are reconciled would appear not to be fully formalized. There are some joint committees, and strong disagreement on a high profile matter could be advanced to the deputy minister.[64] It is unclear how much these processes are leveraged to overcome the identified challenges.

71. (U) Internal silos at NSLAG between the advisory and litigation wings also play a role. These internal silos were reportedly a contributing factor in the confusion and uncertainty surrounding the omission of information in the warrants in 2020 FC 616.[65] Many of the unlawful activities at issue in that case involved sources and operations for which legal advice had been previously discussed within NSLAG in the advisory branch, where relevant opinions on matters such as crown immunity had been produced.[66] However, warrants counsel reportedly were not always aware of this advice. The breakdown of internal silos is thus essential for the avoidance of such sequences of events in the future.

72. (U) Moreover, CSIS's activities are sufficiently unique and unusual to impose a steep learning curve on counsel. This learning curve manifests itself in several ways. First, NSLAG lawyers must become familiar with the unique and classified CSIS operational environment, something that some interviewees on the CSIS side suggested counsel needed to better understand.[67] Second, novel questions may require careful and collective consideration, ensuring that Justice "speaks with one voice" but also slowing the process of delivering advice.[68]

73. (U) Finally, Justice cannot easily overcome the inherent uncertainty of some legal issues,[69] and Justice lawyers may often be obliged to voice legal doubt; that is, the unhelpful "yellow light" concept. Legal doubt is anathema in a rule of law system – it is difficult to ask an organization to comply with a law when that law is unknown. The law in national security can be especially unsettled. The sometimes imprecise statutory law applicable to CSIS is rarely subject to judicial interpretation, creating considerable uncertainties. Meanwhile, case law on section 8 of the *Charter* mostly arises in the criminal law context, and Justice counsel are left to extrapolate from these decisions to the related, but still distinct world of CSIS operations. Often, the sole means to address legal uncertainty is to bring legal questions to the Federal Court through warrant applications.

---

61 Interview(s).
62 Interview(s).
63 Interview(s).
64 Interview(s).
65 Interview(s).
66 Interview(s).
67 Interview(s).
68 Interview(s).
69 Interview(s).

74. (U) In sum, national security law is a highly specialized and constantly developing area. Nonetheless, CSIS needs efficient advice, a need that goes to the heart of both CSIS and Justice's mandates.

2. Reform Initiatives

75. This section addresses recent reform initiatives in the delivery of legal services at Justice.

a. NSLAG's Recent Internal Protocols

76. (U) Justice told NSIRA that it is aware of the need for change in the organizational culture at NSLAG.[70] A new NSLAG Executive Director took office in January 2020 and, since then, has reportedly participated in senior-level discussions with CSIS on cultural change management.[71] NSLAG noted some resistance to change management within its organization, but reported a generally healthy appetite for change,[72] including with an aim of addressing concerns about information silos.[73]

77. (U) NSLAG has implemented several new internal procedures addressing internal silos by facilitating awareness among litigation counsel on emerging legal issues on the advisory side (and presumably vice versa). NSLAG has developed its own classified version of Justipedia to assist with knowledge management, with the aim of ensuring consistent legal opinions.[74] NSLAG holds weekly practice group meetings in which participants provide "roundtable" updates on their work. If a practice group is unable to sort out a legal issue, the matter may escalate through several levels of management within NSLAG, to the Executive Director.[75] While these reforms may assist in bridging internal silos, they may not be sufficient. NSLAG must develop a process whereby there is a method to communicate with, or brief warrant counsel where advice has been provided for an operation that subsequently becomes prioritized for a warrant.

78. (U) Justice sometimes issues practice directions to provide guidance to counsel on certain aspects of their practice. In 2019, Justice issued two practice directions related to the duty of candour in warrant applications. The first specified that warrant applications will not rely on information derived from unlawful activity, and where unlawful activity occurs, it must be brought to the Court's attention.[76] The second provided guidance on information that must be disclosed to the Court, including whether the human source has engaged in illegal activities, as well as issues that inform the credibility and reliability of a source.[77]

---

70 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 8, line 14,

71 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 9, lines 14-17.

72 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 10, lines 9-15.

73 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 10, line 16.

74 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 52, line 2 – p. 53, line 2.

75 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 107, line 23 – p.108, line 9.

76 Issued on on April 18, 2019, pending the [2020 FC 616] decision. The Practice Direction further stated that where there may be doubt as to whether the activity undertaken is unlawful, that activity must be brought to the Court's attention.

77 On Sep 20, 2019, Justice issued a 2nd practice direction, to complement the Apr 2019 one, as well as the Policy of the Department of Justice and CSIS on the Duty of Candour in ex parte Proceedings (Joint Policy). The Sep 2019 practice direction stated that, working together, affiants and counsel must disclose to the Court information, however tenuous, that is material to (a) whether the human source has engaged in activities that could lead to an abuse of process; and (b) the credibility of the source and the reliability of the information provided by the source. It noted that while affiants have the primary responsibility for reviewing the human source file for information relied upon in the warrant application, counsel must engage in an independent, impartial assessment of the information falling into categories (a) and (b), and should review the human source file as appropriate. The Practice Direction instructed both the affiant and counsel to err on the

79. (~~S/C~~) On September 22, 2020, Justice issued a practice note to NSLAG counsel [redacted] [Description of contents of note] [redacted][78]

80. (~~S~~) Not all interviewees thought these changes would suffice to address NSLAG's internal silos, and worried that dots would not be connected between legal advisory opinions and operational legal issues. One suggestion was to ensure that relevant advisory opinions are [IM solution suggested] [redacted][79]

81. (U) Moreover, NSLAG's range of expertise may not suffice to identify every latent legal issue. In addition, those components of Justice with that capacity may not appreciate the nature of CSIS's mandate and operations. Some interviewees urged NSLAG's litigation role needs to be supplemented by working more closely with Justice's general litigation lawyers in their counsel role,[80] requiring that information silos be overcome. NSIRA notes Justice recently implemented tools specific to its national security role. These include a number of DM-level committees that address broad policy and operational matters in national security and which involve other LSUs.[81]

82. (U) NSIRA observes that Justice's capacity to anticipate new issues depends on an alert client. Interviewees described an effort to be more proactive, and to raise to the CSIS Director legal issues requiring proactive resolution.[82] At a minimum, it will be important for the Director to work with Justice and Public Safety Canada to anticipate emerging legal issues, and organize effective means of resolving them.

b. Renewed NSLAG and CSIS Relations

83. (U) NSLAG acknowledged the need "to do a better job ensuring that the client understands the legal landscape".[83] It recognized client frustration with the law in some circumstances, since court cases may provide direction that is sometimes confusing in real world situations, including with respect to *Charter* issues and a person's reasonable expectation of privacy.[84] Although it does conduct some training for CSIS, NSLAG says it could be doing more outreach and engagement.[85] As part of CSIS's Project [redacted][Name][redacted], discussed further below, NSLAG has indicated the need for more outreach training in both directions, including CSIS providing training for NSLAG.[86]

---

side of disclosure, and emphasized the need for a complete and accurate account of the facts rather than presenting CSIS in the best possible light. DoJ, *Practice Direction on the Disclosure of Information regarding Human Sources in Warrant Applications*, Book of Documents (Oct 9, 2020) [TS], Tab 23, pp. 1-2.

78 [redacted] Book of Documents [TS], Tab 25, p. 2.

79 Interview(s).

80 Interview(s).

81 F. Daigle, Briefing Transcript (October 9, 2020) [Protected B], p. 26, line 22 – p. 27, line 14; Department of Justice, "NSLAG Participation on Committees and in Working Groups", Book of Documents [Top Secret], Tab 7.

82 Interview(s).

83 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 23, lines 1-3.

84 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 23, lines 1-25.

85 L. Johnson, Briefing Transcript (October 9, 2020) [Top Secret], p. 24, lines 4-7.

86 Project [redacted] was initiated in response to the Rosenberg report. At the time of writing the project had been integrated into a larger initiative referred to as [redacted] which seeks to "coordinate specific project activities, at a high level, and to identify and manage the organizational benefits each project develops". Ref: [redacted] Programme, [redacted] Update, December 15, 2020.

84. (U) NSLAG also appears to recognize the desire for a different approach to giving advice, including moving toward road map-style legal advice that works collaboratively and iteratively with CSIS to achieve operational goals within the bounds of the law. NSIRA heard that NSLAG regards this approach as a best practice and is committed to it, although it was not clear at the time of the review how far Justice had moved toward a generalized, road map-style form of advice-giving.[87]

85. (U) It was clear, however, that Justice generally does not support a solution of "embedded" legal counsel at CSIS regional offices.[88] Justice interviewees regarded embedding as raising risks of client capture and posing challenges for internal staffing and consistency of advice.[89] Instead, Justice and CSIS have recently launched a pilot project in which specific counsel were designated to support CSIS throughout a specific operational 'mission'.[90]

86. (U) Moreover, NSLAG has piloted an "office hours" practice, relying on headquarters-based counsel serving as liaison counsel for the regions. Those regional liaison counsel who currently provide support make themselves available to the regions to receive informal queries. The office hours initiative was conceived as a means of permitting CSIS personnel to put forth "trial balloons" regarding operational possibilities before possibly formulating a request for formal legal advice, which would then be put through the conventional advice request process.[91]

87. (U) NSIRA also heard that a revamped approach to the giving of advice would require cultural adjustments at both CSIS and Justice. The Justice practice of vetting advice through a hierarchy may be difficult to reconcile with more timely legal involvement.[92] Novel questions may require careful and collective consideration, ensuring that Justice "speaks with one voice" but they will need to be mindful that delay may jeopardize operation or reach a point of uselessness.[93] As noted, short of converting CSIS officers into legal experts, regular and timely access to legal advice is essential to meeting the standards of the rule of law without stymying operations. NSIRA would also note that even formal legal advice will need be geared to the consumer, and thus should avoid legalistic discussions largely meaningless to non-lawyers.[94]

88. (U) In moving toward such a system, NSLAG will need to avoid client capture in order to meet the Attorney General's obligation to honour and advance adherence to the rule of law, while also facilitating CSIS's operational imperatives. A dominant theme of the interviews was the challenge of reconciling the Attorney General's obligation to maintain the rule of law with client-

---

87 Justice Legal Risk Approach, 15 July

88 Interview(s).

89 Interview(s).

90 Source Article, [redacted] A success story in the making, [redacted] 2021. [redacted] Briefing to NSIRA, August 18, 2021.
As of late 2021, this pilot project was expanded to include limited hours for designated counsel for multiple regional offices as well as operational and policy centers. Employees are able to send queries to counsel. CSIS has noted that it is tracking queries through a template which allows for collection of data about the issues employees are seeking advice on to identify trends that can be subsequently addressed through policy and training. Ref: CSIS Factual Accuracy Check, December 22, 2021.
DoJ Briefing (L. Johnson), October 9, 2020; DoJ Briefing (K. Unger), December 18, 2020; DoJ Briefing (D. Robinson), March 16; DoJ Briefing (L. Johnson) July 15, 2021.

91 Interview(s).
[redacted] Briefing to NSIRA, February 18, 2021.
L. Johnson Briefing Transcript (October 9, 2020) [Top Secret] p. 24 lines 8-14; K. Unger Briefing Transcript (December 18, 2020) [Top Secret] p. 52, line 19 - p. 53 line 25, p. 54 lines 1-6, p. 55 lines 11- p. 57, line 1; D. Robinson Briefing Transcript (March 16, 2021) [Top Secret] p. 30 lines 8-16, p. 31 lines 6-25; L. Johnson Briefing Transcript (July 15, 2021) [Top Secret] p. 39 lines 3-23.

92 Interview(s).

93 Interview(s).

94 Interview(s).

centered service delivery models giving clear and consistent legal advice to CSIS in the execution of its lawful mandate. Lawyers do not easily reconcile these objectives, and interviewees were of the view that clearer instruction on the role of the AG and codified standards for giving advice were advisable.[95] Thus, NSIRA heard support for the idea that NSLAG should have advisory service standards.[96] Such standards are especially important if, as NSIRA heard, at the more senior levels in Justice, the border between legal advice and policy advice may begin to blur. Some interviewees indicated that at this level, there can be a strong cultural desire to give the client room to maneuver.[97]

89. (U) For its part, CSIS will need to become more comfortable working closely with legal advisors, and in disclosing the full range of sensitive details needed for Justice counsel to provide useful advice.[98] Generally, CSIS interviewees seemed to welcome the office hours approach, though some noted its usefulness will be dependent on the personality and experience of the counsel, and in any case, it is not a panacea.[99] This reaction highlighted the reservations of some CSIS officers based on past unsatisfactory interactions involving inexperienced counsel.[100]

c. Additional Steps at NSLAG

90. (U) Justice faces, therefore, the ongoing challenge of giving fearless, timely, consistent and clear legal advice while at the same time developing client-centered service models, in an area (national security) that is a niche, often highly-specialized concern for the department and fraught with legal uncertainties.

91. (U) In assessing current initiatives in future reviews, NSIRA will be especially concerned with how Justice embraces a road map-style of advice-giving. Based on the information collected for this review, NSIRA believes that useful advice must be offered during operational planning and execution, a prospect that NSIRA expects the pilot project involving an operational mission will explore. Advice should continue as the operation is evolving in response to unforeseen legal matters requiring immediate guidance. Based on its interviews, NSIRA believes the success of this system will depend on a number of features. First, the optimal delivery of legal services must rely on Justice counsel who are sufficiently experienced and attuned to the unique CSIS operating environment. While not embedded in the regions, it seems these counsel will need to be entrusted with the ability to interact directly with CSIS operational clients at all levels, including during live operations, and give advice on routine matters without delay. These counsel will also need to be familiar with Justice's position on recurring issues so as not to jeopardize the one voice model. To this end, NSLAG would likely benefit from developing a concise reference tool with its position on recurring issues and most common legal authorities invoked and make the tool accessible to counsel to support their real-time advice.

92. (U) Not every legal issue will be routine. Yet, counsel participating in operational planning should be well positioned to anticipate and articulate more difficult legal issues, and then be responsible for resolving these legal questions in keeping with Justice's one voice approach. Counsel involved in operational planning should serve as the entry to Justice for matters requiring additional internal consultation at Justice with either their NSLAG colleagues or those

---

95 Interview(s).
96 Interview(s).
97 Interview(s).
98 Interview(s).
99 Interview(s).
100 Interview(s).

in centres of expertise. A counsel fully apprised of operational realities who is able to "case-manage" the provision of advice in this manner may avoid the problems of "broken telephone" and non-responsive legal advice associated with the conventional advice-giving model.

93. (U) Legal involvement in CSIS activities, as they are being planned and organized, should also allow Justice to provide informal legal nudges that allow CSIS to course-correct before too much time has been spent. Closer legal involvement during the early phases will minimize the need for legal opinions on operations that are late in the development cycle or that are already underway.[101] Put another way, a more iterative process of incorporating legal advice over the full course of an operation could address the reported challenge of operations halted due to untimely or ambiguous legal advice.

94. (U) Critically, meeting these objectives requires CSIS to invite Justice counsel to sit at the table at all stages of the lifecycle of an operation, and for Justice counsel to be fully and frankly briefed on operational objectives, intent, and details.

d. Broader Department of Justice

95. (U) Justice has embarked on a "transformational change" initiative, in consultation with clients, to improve how it conducts its work and supports its clients. Launched in 2018, the VISION comprises four pillars: meaningful risk assessments; client-centric strategic partnerships; recognizing and building expertise; and, simplifying the funding model.[102] One of the key priorities includes an overhaul of the existing Legal Risk Management Framework,[103] which Justice has recognized for some time does not effectively communicate risk.[104]

96. (U) Interviewees made clear that Justice's manner of characterizing legal risk in the Legal Risk Management (LRM) Framework is not understood in the same way by its lawyers and its clients and is not always regarded as useful even by the lawyers applying it.[105] For instance, something that is "high legal risk" is very likely unlawful under the LRM Framework, but this was not always understood by clients. Justice did not provide NSIRA with the full draft revised LRM Framework as modified in the context of VISION, as it is still under development. Justice did however provide and brief NSIRA on some working LRM documents. On the basis of these materials and briefings, NSIRA believes that two [aspects relating to the LRM Framework] need to be addressed.

97. (U) First, there will be instances in giving advice where Justice should describe activity not as "high risk", but simply as unlawful. Certain legal questions can be answered unequivocally, even accounting for the cautious nature of lawyerly advice. In a system based on the rule of law, and given the role of the Attorney General, such questions should be answered in as definitive a manner as possible. That there may be some hypothetical possibility that the activity might not be unlawful does not mean that Justice should fall back only on the language of "high risk", since this phrase may give a client the impression such activities, while "risky", are still a viable option for risk-embracing officials. Justice should avoid such situations. Where an activity is very likely unlawful, Justice should tell the client exactly that and describe the

---

101 Justice Legal Risk Approach, 15 July; Interview(s).
102 Department of Justice, "About the Vision", Book of Documents (October 9, 2020) [Protected B], Tab 6, p. 1.
103 The current framework was implemented in 2013-2014. A. Saranchuk, Briefing Transcript (October 9, 2020), p. 70.
104 Justice had been updating the LRM Framework prior to 2020 FC 616, and the process has been further informed by the decision. F. Daigle, Briefing Transcript (October 9, 2020) [Protected B], p. 24.
105 Interview(s).

consequences of proceeding, rather than simply couch its conclusions in a probabilistic formula.

98. ~~(S/C)~~ Some interviewees underscored this view in discussions with NSIRA.[106] Further, NSIRA notes that Justice has proposed [discussion of Justice initative]

99. ~~(S/C)~~ [Discussion of operational aspects and purpose of Justice initative]

---

106 Interview(s).

107 Justice,

108 Department of Justice, Book of Documents (October 9, 2020) [Protected B], Tab 16.

109 Department of Justice, [Protected B], Tab 17.

110 Specifically, offences under the *Criminal Code of Canada* or another statute. *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*; and *Controlled Drugs and Substances Act*. Department of Justice, Book of Documents (October 9, 2020) [Prot B], Tab 17, pp. 1-2, see also footnote 4.

111 Department of Justice, Book of Documents (October 9, 2020) [Prot B], Tab 17, p. 2.

112 Department of Justice, , Book of Documents (July 15, 2021) [Protected B], Tab 3.

113 Department of Justice Book of Documents (July 15, 2021) [Protected B], Tab 3, p. 4.

114 Department of Justice, Book of Documents (July 15, 2021) [Protected B], Tab 3, p. 2.

115 Department of Justice, Book of Documents (July 15, 2021) [Protected B], Tab 3, p. 3.

[redacted][116][redacted]

[redacted][117]

100. (U) In contrast, [discussion of an NSIRA perceived gap in Justice initative] [redacted][118] [redacted][119] In NSIRA's view, this approach is not sufficiently robust. [Discussion of NSIRA's recommended approach to address the identified gap] [redacted]

101. (U) Second, NSIRA notes that many of the [description of certain aspects of Justice's tools] [redacted] NSIRA regards these considerations as inappropriate, [discussion of the Justice approach] [redacted]. In a system based on the rule of law, [discussion of using such an approach] [redacted] [Discussion of using an approach and the risks of that approach] [redacted] [Discussion of certain legal tools] [redacted][120]

102. (U) Justice believes that the draft [discussion of aspects of Justice initative] [redacted]

103. (U) Still, without careful mitigation, NSIRA believes that there remains a risk [redacted] [discussion of a concern relating to Justice initative] [redacted]

104. (U) In sum, based on the role of the AG in advancing the rule of law, [redacted]

---

116 Department of Justice, [redacted] Book of Documents (July 15, 2021) [Protected B], Tab 3, pp. 5-6.

117 Department of Justice, [redacted], Book of Documents (July 15, 2021) [Protected B], Tab 3, p. 3.

118 The [redacted] See Department of Justice, [redacted] Book of Documents (July 15, 2021) [Top Secret if Tab 4 included], Tab 3.

119 Briefing, Justice Legal Risk Management, 15 July, 2021.

120 Interview(s).

[discussion of a standard to address the identified concern in the Justice initative] In future reviews implicating Justice's legal advice, NSIRA will be attentive to whether advice meets this standard.

105. **Finding no. 1: NSIRA finds that the legal advice-seeking and giving process, and resource constraints at NSLAG, contribute to considerable delays,** [description of timeline]

106. **Finding no. 2: NSIRA finds that Justice legal opinions have sometimes been prepared without sufficient attention to the audience that needs to understand and act on them. Opinions have been focused on assessing legal risk, often late in the development of a CSIS activity, with limited effort made to propose alternative and legally sustainable means of arriving at the intended objective.**

107. **Finding no. 3: NSIRA finds that the Justice Legal Risk Management Framework is misunderstood at the working level at CSIS and that it does not provide an appropriate framework for the unequivocal communication of unlawful conduct to CSIS.**

108. **Finding no. 4: NSIRA finds that difficulties in acquiring prompt and relevant legal advice have contributed to the** [discussion of the detrimental effects on and risks to operations] **that may require legal advice. In consequence, the manner in which Justice has provided legal advice to CSIS does not always meet the needs of CSIS operations.**

109. **Finding no. 5: NSIRA finds that Justice does not generate the necessary business analytics to track its service delivery performance to CSIS.**

110. **Finding no. 6: NSIRA finds that Justice has acknowledged that internal silos at NSLAG between the advisory and litigation wings have sometimes left warrant counsel unaware of emerging legal issues and that Justice has taken steps to resolve these issues.**

111. **Finding no. 7: NSIRA finds that Justice has committed to improve its advice giving to CSIS, including moving toward "road map" style legal advice that involves working collaboratively and iteratively with CSIS to achieve operational goals within the bounds of the law.**

112. **Finding no. 8: NSIRA finds that CSIS has not always shared all relevant information with NSLAG, prompting a degree of mistrust and limiting Justice's ability to provide responsive legal advice.**

In view of these findings, NSIRA recommends that:

(U) Recommendation no. 1: Justice pursue its commitment to reforming the manner of providing legal advice to CSIS, and its stated commitment to "road-map" style advice as a best practice. In support of this objective and the provision of timely, operationally relevant advice, NSIRA further recommends that Justice implement the following:

- **Whether through an expanded office hours or liaison counsel program or otherwise, NSLAG must develop a legal support service operating full time, staffed by experienced lawyers empowered to provide operational advice in real time on which CSIS officers can rely, on the basis of settled Justice positions on recurring legal issues, accessible directly to CSIS officers across all regional offices and at all levels.**

- **NSLAG develop a concise reference tool with its position on recurring issues and most common legal authorities invoked and make the tool accessible to counsel to support their real-time advice.**

- **To minimize the need to resort to the formalized legal advice-seeking process, NSLAG (in coordination with CSIS) must involve counsel with CSIS officers at the early stage of the planning of key or novel operations and throughout their entire operational lifecycle to case manage an iterative legal guidance process.**

(U) Recommendation no. 2: NSLAG (in coordination with CSIS) develop Key Performance Indicators to measure the delivery of legal services to CSIS.

(U) Recommendation no. 3: CSIS and Justice include in their training programs interactive scenario-based training developing the operational intelligence activities expertise of NSLAG counsel and the legal knowledge of CSIS operational staff.

(U) Recommendation no. 4: To ensure Justice is able to give meaningful and responsive legal advice as recommended in recommendation #1, that CSIS invite Justice counsel to sit at the table at all stages of the lifecycle of key and novel operations, and that it fully and frankly brief counsel on operational objectives, intent, and details.

(U) Recommendation no. 5: Justice's advice giving must clearly and unequivocally communicate advice on the unlawfulness of client conduct, whether criminal or otherwise.

B. Warrant Process

113. (U) While the preceding section dealt with issues related to the provision of legal advice in the course of all of CSIS operations, the current warrant process is fraught with its own problems, as illustrated by numerous Federal Court decisions.

114. (U) Warrants are critical to CSIS's success as an intelligence service. [redacted] [Discussion of prior internal review] [redacted] "The information obtained through their execution is the Service's lifeblood".[121] At the same time, another, more recent review concluded that for many within CSIS, the warrant process is regarded as a "necessary evil" on account of its onerousness.[122] This section examines the "warrants life cycle", from prioritization to execution, in order to identify and assess the underlying factors that have made CSIS's warrant process cumbersome.

1. Basic Legal Rules

115. (U) Section 21 of the *CSIS Act* provides the basic rules for warrant applications. If CSIS believes on reasonable grounds that a warrant is required to enable it to investigate a threat to the security of Canada (or collect foreign intelligence for section.16 purposes), it may, with the approval of the Minister, make an application to the Federal Court for a warrant. The affidavit supporting the application must provide the supporting facts demonstrating the reasonable grounds to believe that a warrant is needed to investigate the threat.

116. (U) In practice, CSIS organizes the process of seeking a warrant around a system of internal preparation and approvals before proceeding to the statutory step of seeking ministerial approval of the warrant application. In order to understand fully the warrant process, NSIRA has broken it down into several stages of a larger "warrant lifecycle", each of which are discussed below.

117. (U) A number of legal concepts and expectations enter into the warrant process, including, in particular, the "duty of candour" owed to the Court. As noted, warrant proceedings are conducted in the absence of the target and are closed to the public in order to protect the covert nature of a search. To compensate, however, for the one-sided nature of such proceedings, courts (and the law societies that regulate the legal profession) impose elevated obligations of candour on the lawyers and party appearing before the court, also known as a duty of utmost good faith.[123] The evidence presented by the party "must be complete and thorough and no relevant information adverse to the interest of the party must be withheld."[124] In consequence, the party must "conduct a thorough review of the information in its possession and make representations based on all of the information including that which is unfavourable to their case."[125]

---

121 [redacted]

122 M.Rosenberg. Independent Review: Duty of Candour at CSIS, 2020 03 03, Slide 5.

123 Ruby v Canada, 2002 SCC at para 27.

124 Canada v Harkat, 2014 SCC 37 at para 101.

125 Ibid at para 101. See also Almrei (re), 2009 FC 1263 at para 500.

118. (U) The concept of "materiality" guides which facts must be disclosed to the court. Thus, in CSIS warrant applications, CSIS "must present all material facts, favourable or otherwise".[126] "Materiality" simply means a fact relevant to an issue in the case. For CSIS warrants, "information is material if it is relevant to the determination a judge must make in deciding whether or not to issue a warrant, and if so, on what terms."[127] For instance, a material fact is one that is relevant to "the belief, on reasonable grounds, that a warrant… is required to enable" CSIS to investigate a threat to the security of Canada.

119. (U) The Federal Court has held, however, that materiality extends beyond facts relevant to the factors expressly listed in section 21 of the CSIS Act. For instance, materiality reaches "information about the broader framework in which applications for the issuance of CSIS Act warrants are brought".[128] This means the duty of candour includes information that is "material to the judicial exercise of discretion" to issue a warrant.[129] It includes the flagging of "legal issues that could be of concern to the Court".[130] Legal issues do not, however, exhaust this broader category of materiality, as it also reaches disclosure of CSIS's precise conduct under a warrant that may influence the Court's exercise of discretion.[131]

120. (U) This broader category of "material to the exercise of discretion" relates to the especially important role of the Federal Court as the primary source of independent control over CSIS activities conducted under warrant. Unlike a police warrant, which may be retrospectively scrutinized by a second judge in adversarial proceedings if a police investigation culminates in a prosecution, the Federal Court judge is often the only judge who ever examines a CSIS warrant. The target of the warrant or the broader public will usually never know the CSIS activities conducted under the authority of that warrant. In this context, the Federal Court has signaled a redoubled urgency to meeting a broad duty of candour.[132]

121. (U) It is clear, however, from our interviews, that the broad conception of materiality has led to doubt and confusion within NSLAG and thus within CSIS. Those interviewees who addressed the issue appeared to agree that Federal Court candour concerns now fit into (at minimum) two categories, which we define as "material to credibility", and "material to matters of potential concern". NSIRA defines these categories as follows:

- Material to Credibility: Facts relevant to an express statutory threshold that the court is asked to assess, most notably the statutory standards judges consider in issuing warrants. This category includes, especially, information that goes to the credibility of the sources whose information supports the warrant application.[133]
- Material to Matters of Potential Concern: Facts or legal issues concerning those aspects of the CSIS activity that might be unusual (or unanticipated) and that a judge will wish to know in exercising their discretion to issue a warrant and in imposing associated conditions. This category includes, for example, a failure to disclose tradecraft conducted to gather

---

126 X (Re), 2013 FC 1275 at para 83, aff'd 2014 FCA 249.
127 2021 FCA 92 at para 127.
128 X (Re), 2013 FC 1275 at para 89, aff'd 2014 FCA 249.
129 X (Re), 2014 FCA 249 at 61; Crown Immunity Case, FCA at para 131-133.
130 2021 FCA 92 at paras 137 and para 140.
131 X (Re), 2013 FC 1275 at para 89, aff'd 2014 FCA 249 (failure to disclose that CSIS was leveraging CSE's assistance mandate and relationship with Five Eyes partners to conduct the intrusive collection); Associated Data, 2016 FC 1105 (failure to disclose that metadata collected incidentally under warrant was retained by CSIS).
132 2021 FCA 92 at para 124-126.
133 See, e.g., Peshdary v Canada, 2018 FC 911; Almrei (Re), 2009 FC 1263 at para 500; [Brown decision]

information supporting the warrant that may constitute illegal activity[134], the failure to disclose conduct under a warrant that might result in information sharing with other agencies, potentially imperiling the target,[135] or circumstances in which the warrant will be implemented and that may not be obvious in the application.

122. (U) The first category of materiality should be well understood by CSIS and its lawyers. The contours of the second category are not as easily determined and require careful consideration by Justice counsel, assisted by a professional cadre of affiants who reach out to regions to determine how warrants will be executed.[136]

2. Historical Initiatives

123. (U) As outlined in Annex A, incidents concerning CSIS's observance of its duty of candour are almost as old as CSIS. Following each failure, CSIS Directors promised reforms. CSIS introduced new policies, but problems recurred.[137] In other words, repeatedly, progress has been made on paper, but without genuinely correcting the underlying problems. CSIS appears to have a long history of quick reforms, followed by neglect, high turnover of personnel leading to a loss of institutional knowledge, and resourcing that did not match stated priorities.[138] Some interviewees described reforms as typically focused on the minutiae of process rather than on achieving measurable outcomes.[139] CSIS does not track or measure the success of past reforms.[140] In the eyes of some, CSIS reforms often represented "band-aid" solutions rather than attempts to get to the core of issues, and often resulted in the creation of new bureaucracy.[141] In NSIRA's view, CSIS's chief challenge is to break this cycle.

124. **Finding no. 9: NSIRA finds that CSIS has a history of quick reforms, followed by neglect, high turnover of personnel leading to a loss of institutional knowledge, and resourcing that did not match stated priorities. CSIS does not track or measure the outcome of past reforms adequately and has no performance metrics for assessing success.**

3. Description of the Warrant Process

125. (U) NSIRA notes that even determining how the warrants process works presents challenges. Internally, warrant requirements are not adequately codified in applicable policy. CSIS policies have not kept pace with operational reality, as they are often vague, dated, overlapping and contradictory.[142] The gap in policy was evident when examining the warrants policies, which were last updated in 2018 prior to the warrant process undergoing substantial changes, including the implementation of the Affiant Unit (AU) in 2019.[143] Given these issues, a basic

---

134 2020 FC 616

135 X (Re), 2013 FC 1275 at para 89, aff'd 2014 FCA 249 (failure to disclose that CSIS was leveraging CSE's assistance mandate and relationship with Five Eyes partners to conduct the intrusive collection)

136 Interview(s).

137 Interview(s).

138 Interview(s).

139 Interview(s).

140 Interview(s).

141 Interview(s).

142 Interview(s).

143 RFI 4- Warrants Acquisition Guidelines, 2021 08 06 (*Received 2021 08 26).*

question that arises is whether those CSIS officers conducting investigations are sufficiently attuned to when the law requires a warrant.

126. (U) NSIRA heard that there is a clear threshold for when a warrant process must typically be initiated for well-established collection techniques.[144] However, absent clear policy, there was more legal doubt when at issue was the use of novel technologies with uncertain legal ramifications and requirements.

a. Prioritization of Investigations for Warrants

127. (U) Once a region or desk has identified the need for a warrant, the first step in the process is the internal prioritization at CSIS of a target case file or investigation for a warrant application. In practice, this prioritization amounts to a system of triage, assigning limited warrant application resources to specific files. However, it was evident to NSIRA that CSIS employees involved in the warrants process had little to no common understanding regarding the process or basis on which a warrant is prioritized.[145] Even senior officials in the CSIS hierarchy regarded the prioritization process as a mystery.[146]

128. (U) NSIRA heard that headquarters prioritization standards remain a work in progress, and sometimes a struggle among competing interests.[147] The DDO meets weekly with a number of CSIS executives to discuss the investigations requesting a warrant and the possible operational, legal or process developments that could affect priorities for decision-making on warrants prioritization.[148] While NSIRA was informed that there is a record of decision produced after each prioritization meeting, it remains unclear what criteria are used to prioritize a warrant. Some information suggested prioritization has focused on security-related issues.[149] Others speculated that prioritization also considered the perceived amount of work, availability of lawyers and affiants, and how long it would be until current warrant powers expired and needed renewal.[150] Frequent shifts in this process of prioritization have reportedly produced situations where a warrant process starts and stops several times, wasting precious time and adding to operational uncertainty.

129. (U) Given the complexity and lack of clarity of the prioritization process, it has been very difficult to bring novel issues to the Court with the goal of addressing legal ambiguities through court decisions.[151] NSIRA heard about activities that [discussion of detrimental effects on operations] over unresolved questions of law that could have been addressed by the Court. There appeared to be agreement among our interviewees that more matters should be taken to court – and whenever in doubt, seek a warrant.[152]

130. (U) Given the current situation, however, NSIRA's impression is that for CSIS to take a legal issue to Court likely requires the combination of a high priority investigation and the existence of just the right real-world scenario to illustrate the legal issue. Of course, any attempt to resolve legal uncertainty runs the risk of obtaining a legal ruling that constrains rather than

144 Interview(s).
145 Interview(s)., The Warrant Life Cycle -Affiant Unit Briefing December 4, 2020 & February 22, 2021
146 Interview(s).
147 Interview(s).
148 CSIS Response to RFI 3.
149 Interview(s).
150 Interview(s).
151 Interview(s).
152 Interview(s).

empowers investigations. NSIRA heard from some interviewees that there may be a reluctance to take issues to court as there is always a risk of obtaining the "wrong answer".[153]

131. **Finding no. 10: NSIRA finds that CSIS policies have not kept pace with operational reality, as they are often vague, dated, overlapping and contradictory. The absence of clear policy creates legal doubt or concerns, and gives rise to disparate interpretations of legal and operational standards.**

132. **Finding no. 11: NSIRA finds that there is little common understanding regarding the process or basis on which a warrant is prioritized. Frequent shifts in this process of prioritization have added to operational uncertainty. The prioritization process has made it very difficult to bring novel issues to the Court with the goal of addressing legal ambiguities through court decisions.**

Recommendation no. 6: NSIRA recommends that CSIS adopt, and share internally, clear criteria for the warrant prioritization process.

b. The Complexity of the Warrant Acquisition Process

133. ~~(S/C)~~ Once CSIS decides to prioritize a warrant application for an investigation/case, CSIS begins the warrant acquisition process. This process has always been lengthy and bureaucratic. In 1992, the Honourable George Addy reviewed the CSIS warrant process and reported [redacted] steps spanning a total of [redacted] and involving from [redacted] people. Approximately [redacted] people knew the identity of the target before the warrant was issued, seemingly undercutting the "need to know" principle. George Addy commented adversely on the length of the warrant process. He wrote: "[w]hatever procedures might finally be decided upon, it is of paramount importance that, from the moment the decision to initiate the process is taken, the time required to obtain a warrant should never exceed [redacted], as an absolute maximum."[154]

134. (~~S/C~~) Yet, [redacted][155]

135. ~~(S)~~ At present, according to the documents provided to NSIRA, the process involves [redacted] administrative steps in a security intelligence warrant request, [redacted] which are internal to CSIS and Justice prior to the application's filing at the Federal Court.[156] For a foreign intelligence warrant, there [redacted] steps. The timetable for the renewal of a security intelligence warrant anticipates a process of [redacted] working days, or [redacted] (Annex B).[157] The process involves [redacted] committees or units within CSIS (and possibly more if the warrant implicates more

---

153 Interview(s).

154 Study of, Report on, and Recommendations Relating to Process for Acquisition of Warrants by CSIS, George Addy. 1992

155 [redacted]

156 CSIS Doc [redacted] A new security intelligence warrant has [redacted] fewer steps, and appears to be approximately [redacted] shorter. Scheduling documents for a 2020 renewal of a [redacted] security intelligence warrant anticipates [redacted] steps [redacted]

157 RFI 4 (See Annex B)- this timeframe is the designated time frame for routine warrants, it is longer for [redacted] warrants [redacted] and shorter for urgent or fast tracked warrants.

than one region), NSLAG, and Public Safety Canada. At least [Number] CSIS managers are named in the process, as are [Number] Justice employees and the Minister and Deputy Minister of Public Safety.

136. (U) NSIRA was unable to find any one person who could describe precisely the rationale of each of these [multiple] of steps in the overarching scheme; even those close to the process were not always sure what role each approval step played.[158] Few of the steps are mandated by law, but rather they appear to have accrued over time despite repeated efforts at streamlining. Some steps appear to reflect older reform efforts triggered by concerns over compliance, not least with the duty of candour. And yet, as noted at the outset of this review, the candour issues at CSIS persist.

137. (U) In sum, the warrant process appears to be caught in a vicious cycle whereby duty of candour failures (or the fear of prospective failures) cause CSIS to add more bureaucratic fixes, which complicate an already lengthy and inefficient process without actually resolving the underlying issues that led to the duty of candour failures in the first place. Indeed, as discussed below, the complexity of the warrant process appears itself to contribute to CSIS's candour issues. CSIS and Justice must break this cycle. A description of how best to do this will first require further discussion of the warrant process itself.

c. The Key Steps in the Process

138. (U) CSIS maintains five categories of warrant applications, the most common of which are new warrants, replacement of existing warrants[159], and supplemental warrants. Each category has its initiating procedures.[160] In all applications, the relevant desk at headquarters and the implicated CSIS operational region conducting the investigation prepare a [redacted][161] [contents of the document] [redacted][162] Together, the [Number] documents detail the threat, the targets, and set out the investigative powers CSIS proposes to use. Once approved, CSIS sends the [document] to NSLAG for a "threshold" determination; i.e., an assessment of whether there are reasonable grounds to believe that a warrant is required to investigate the threat. If NSLAG concludes that the proposed targets meet the threshold, then development of the rest of the warrant application begins. The key contributors to this process are the Affiant Unit, NSLAG and the Warrant Administration Unit.[163]

139. (U) The Affiant Unit (with the advice and legal support of NSLAG) is responsible for preparing the affidavit used in support of the warrant application. The affidavit is the affiant's sworn written testimony and includes a range of information required pursuant to section 21 of the *CSIS Act.* The affidavit is often laid out as follows[164].

---

158 Interview(s).

159 *Ibid*

160 At CSIS this is often referred to as a warrant renewal. However as it necessitates filing a new application rather than a *CSIS Act s.22* renewal application, we have used the more precise internal terminology of replacement. A request for a new warrant will be sent internally to the [Name] [redacted] Branch Headquarters (HQ) or the regions, at which point it will be added to the prioritization list. The replacement of existing warrants is initiated through a call letter sent out by HQ to the regions enquiring if they seek to have the existing warrants replaced (once expired) for another year.

161 [redacted] is the operational desk responsible for the investigation involving the target for whom the warrant is sought.

162 CSIS briefing to NSIRA, Warrant briefing, September 9, 2020.

163 Also known as the [redacted] [Name] Unit [Name] this unit's primary function is the coordination of the warrant acquisition process including organizing all the requisite meetings with those implicated in the process.

164 [redacted]

- Part 1 – Introduction: this section outlines the affiant's work experience and introduces the sources of information and the exhibits used in the application.
- Part 2 – The threat: this section provides information regarding the broader threat and how it relates to CSIS's investigation and the specific list of target(s).
- Part 3 – The subjects of the investigation: this section includes a thorough explanation of the threat posed by each target, based on information from human sources and other operational reporting.
- Part 4 – Powers sought: this section describes the non-warranted (that is pre- or without the need for a warrant) investigative techniques used in the investigation thus far, as well as the powers requested in the application.
- Part 5 – Other matters: this section includes the duration for which the warrant is sought as well as the required consultation with the Deputy Minister and Minister as per subsections 7(2) and 21(1) of the *CSIS Act*.

140. (~~S~~) The affidavit will also include a number of exhibits, the most important of which are the human source précis and the foreign agency précis.[165] The human source précis is a summary of information from CSIS's files that allows the court to assess the reliability and credibility of the human source without revealing the source's identity. It comprises information pertaining to the source's relationship with CSIS, [description of information] and motivation. The précis will also include a corroboration table used to support the source information contained in the affidavit. Where the application relies on information supplied by a foreign agency, the foreign agency précis includes background information regarding the mandate of that agency, the agency's history with CSIS, and whether the information relied upon in the application may have been obtained as a result of mistreatment.[166]

141. (U) Once approved and reviewed in keeping with several additional steps, including the Independent Counsel vetting discussed below, the application goes before the Warrant Review Committee (WRC) for approval. The committee comprises senior members of CSIS and the department of Public Safety Canada as well as observers from other government agencies such as CSE and the RCMP.[167] At the WRC, the affiant provides a brief overview of the investigation, the application is discussed, and a decision is made regarding whether to proceed with the application, and if so, what changes are required. The application is then submitted to Public Safety Canada, where it is reviewed and passed to the Minister accompanied by a summary and advice as to whether the Minister should approve the application. Once approved, Justice files the warrant application package in court on behalf of CSIS.

4. Observations on the Warrant Process

a. A Lengthy, Bureaucratic Process

142. (U) The complexity of the CSIS warrant acquisition process is quite unlike the manner in which the police obtain their search warrants. The length of the process itself can pose

---

165 Exhibits will encompass of a number of other documents such as those exhibits containing information required under the CSIS Act, i.e. the actual warrants sought, the previous s.21 applications pertaining to the same target, the Minister's designation and approval, as well as the Vanweenans list (persons whose communications may be intercepted) and any other document that needs to be brought to the courts attention.

166 [redacted]

167 REF: pg. [redacted]

operational risks, [it may affect the warrant] [redacted].[168]

143. (U) There are reasons why CSIS warrants are more administratively burdensome. Unlike police investigations, CSIS investigations rarely produce evidence culminating in criminal proceedings in court. They thus lack the prospect of retrospective challenge by a party with a vested interest in testing the propriety of the warrant. The safeguards in the CSIS warrant context are therefore prospective, and properly include a careful bureaucratic vetting, as well as executive control exercised by the Minister of Public Safety and judicial control by the Federal Court. Certain steps, such as the Warrant Review Committee, discussed further below, are therefore desirable. However, beyond a certain point, more steps does not correlate with better quality. Indeed, NSIRA observed that many of the steps in the warrant process amount to a series of minor tweaks and clerical changes[169] of limited importance to an application that often becomes an exercise in 'drafting by committee'.[170] What the proliferation of steps has done, however, is to create a process widely regarded as slow and unwieldy, with no clear lines of accountability.

144. (U) For many of our interviewees, the process had the following features:

- Lack of clear accountability due to the proliferation of approvals: Some interviewees described the multiplicity of approvals as a symptom of a broader CSIS culture in which responsibility is diffused, ensuring that the locus of responsibility is never clear.[171] Put more strongly, some interviewees saw the proliferation of approvals as reflective of a risk-averse culture in which officials employ a 'safety in numbers' approach to decisions and sign-offs.[172] In this model, no individual is personally accountable; rather, accountability is diffused throughout the institution.[173] Senior management disputed this characterization noting their support for the concept of shared accountability through approvals.[174] Even so, there did not appear to be disagreement that accountability could be better defined.[175]

- Privileging sign-offs over substance: The long list of approvals over the course of the warrant process consume time; each level of approval means a pause in the work, meaning that the time available to do the substantive work of preparing the warrant application is often squeezed. Since it is not always clear what function each step performs, it is difficult to disaggregate substantive steps from various forms of managerial review, approval and vetting. However, by NSIRA's estimate, only [timeline] [redacted] associated with a warrant (renewal) application involve core substantive work. Many interviewees across varying levels favoured prioritizing time spent on preparation over that spent on managerial approvals.[176] Although recent attempts to streamline the process have resulted in several steps being conducted concurrently, there is little indication that the time saved was reallocated to the preparation of the most complex portions of the application, such as the human source précis.[177]

- A process of black boxes: The warrant process involves a large number of people. Officials

---

168 Interview(s); for different view, discounting that this is a real issue, see Interview(s).
169 Interview(s).
170 Interview(s).
171 Interview(s).
172 Interview(s).
173 Interview(s).
174 [redacted] Briefing, February 22, 2021.
175 Interview(s).
176 Interview(s).
177 RFI 4- warrant schedule, Annex B

implicated at each stage often seemed unfamiliar with decisions made at other stages or the rationales for these decisions.[178] Put another way, each official understood their piece of the puzzle, but had little sense of how the various pieces fit together. There appeared to be few (if any) regular feedback loops, in which explanations for decisions made at one level filtered back to other levels. This tendency to keep information 'siloed' meant that many employees felt that their knowledge of the warrant process was not as good as it should have been and wanted greater visibility on the process as a whole.[179]

- Lack of regional involvement: The 'silo' or 'black box' approach is most galling to the regional investigators. Even though the warrant requests originate from the regions and are made to support regional investigations, [180] operational officials in the regions often have a very limited role in the warrant process. Some requests move forward and others do not, but it is not clear why. When warrants come up for renewal, NSIRA was told that headquarters has not typically sought input from the regions on new collection techniques,[181] and that regions have struggled to obtain modifications in subsequent iterations of warrants to ensure that the warrant reflects operational needs.[182] Interviewees regularly advanced the argument for feedback to and closer engagement with the regions (including on technical matters) throughout the warrant application.[183] The region is best placed to flag issues of concern with the investigation and the sources involved, issues that could be important to the Court. To this end, NSIRA notes that the affidavit and source précis should be regularly shared with the source handler in the region.[184] Likewise, the region should be consulted throughout the warrant application process, and should be represented at the Warrant Review Committee.

- Excessive warrant scope and scale: One matter of concern was the sheer length of some of the affidavits CSIS has put forward in support of warrant applications. This was most pronounced in [type] warrants where requests are made in support of multiple investigations under one application. A related issue is CSIS's tendency to include requests for a wide range of investigative techniques, regardless of whether there was an actual plan to employ them. This appears to be done on the theory that it was prudent to seek all possible powers rather than risk needing to return to court later on – particularly given the amount of time that such a process would involve. An alternative approach is more targeted and streamlined warrant applications, done in greater number and on a predictable annual schedule. This reform was repeatedly favoured in our interviews.[185] Of course, this approach will only succeed if a higher number of warrant applications does not produce more warrant applications of the same length and complexity of the [type] warrants. If the administrative burden of approvals associated with the present system is applied to more warrants, it seems unlikely the system will work. That is, this reform may only succeed by relaxing what was described to us as a "one size fits all" approach to warrant applications, with length and complexity unconnected to the scale or degree of intrusiveness of the techniques at issue.[186]

---

178 Interview(s).
179 Interview(s).
180 Interview(s).
181 Interview(s).
182 Interview(s).
183 Interview(s).
184 Interview(s).
The Warrant Life Cycle -Affiant Unit Briefing December 4, 2020 & February 22, 2021
185 Specifically, large annual warrants might usefully be segmented into smaller more discrete warrants staggered through the year. This staggered schedule would allow unexpected issues arising in investigations to often be dropped into the next scheduled warrant, ideally eliminating the need for supplemental warrants sought during the lifetime of the existing large, Interview(s).
186 Interview(s).

145. (U) NSIRA is therefore of the view that there are significant changes that CSIS could make that would materially improve the quality of warrant applications. NSIRA does not think that the bureaucratization of the CSIS warrant process as described above has improved matters; on the contrary, the lack of clear accountability, lack of internal communication, and excessive complexity have all contributed to the problems facing the process. NSIRA agrees fully with the view that time should be reallocated to those stages that make for a better warrant, including regular engagement with the regions.

146. (U) The warrant process should not be mired in steps that amount to the shuffling of paper between desks. These should either be eliminated, or conducted concurrently with more substantively meaningful steps, avoiding the reality or perception of *pro forma* involvement by officials who lack a clear and manifest need for involvement in the warrants process. Put another way, where there are steps that do not make a significant contribution to a more *accurate* application, CSIS should eliminate them.

147. **Finding no.12: NSIRA finds that the actors involved in the warrant process do not have a common understanding of the rationale for each of the [multiple] steps in the overarching warrant application scheme and are not always sure what role each approval step plays.**

148. **Finding no. 13: NSIRA finds that the proliferation of process in seeking warrants has created a system of diluted accountability widely regarded as slow and unwieldy, with delays caused by multiple levels of approval.**

149. **Finding no. 14: NSIRA finds there is no regular feedback process in which explanations for warrant-related decisions made at one level filter back to other levels. The absence of feedback is especially acute for the regional investigators.**

150. **Finding no. 15: NSIRA finds that often, the sole means to address legal uncertainty is to bring legal questions to the Federal Court through warrant applications. In consequence, an unwieldy warrant process makes resolution of legal doubt more difficult.**

In view of these findings, with respect to the warrant process, NSIRA recommends that:

Recommendation no. 7: CSIS establish a new warrant process eliminating steps that do not make a significant contribution to a more accurate application. The process should assign clear lines of responsibility for the production of accurate applications. The reformed system should ensure that delays associated with managerial approvals are minimized, and that time is reallocated to those steps contributing to the preparation of the accurate applications.

Recommendation no. 8: CSIS integrate the regional stakeholders (including the implicated investigators) at every key milestone of the warrants process.

Recommendation no. 9: CSIS adopt policies and procedures governing the reformed warrant process that clearly outlines the roles and responsibilities of each participant and the objective of each step in the warrant process and that these policies be kept current as the process evolves.

b. Incomplete Knowledge Management in the Regions

151. (U) When discussing the warrant process, NSIRA often asked who should be responsible for the accuracy and completeness of the warrant application. There are two clear points of responsibility. First, staff in the regional offices conducting investigations are responsible for feeding complete, correct and appropriately contextualized information into the warrant production process.[187] Second, the individual most responsible for the final product is the affiant, whose sworn affidavit supports the warrant application and supplies the factual basis permitting the Court to conclude that the legal requirements for the issuance of a warrant have been met.[188] After all, if there is to be a duty of candour failure, it will be because of an inadequate affidavit. Meeting these obligations is, however, unnecessarily difficult for both the regions and the affiant, for the reasons below.

152. (U) CSIS warrant applications often depend on information collected from confidential human sources. As discussed above, the reliability of this information – and the credibility of the source – constitute key material facts in warrant applications. A failure to apprise the court of information relating to credibility is a clear violation of the duty of candour.

153. (U) As noted, source information appears in the warrant application through the source précis and affidavit. The source précis and affidavit, in turn, stem from information that was originally collected by the regions, which handle human sources. In practice, therefore, the affidavit is no better than the quality of the information provided by the regions. If that information is incomplete, none of the [multiple] steps in the CSIS warrant acquisition process can compensate. Notably, omissions regarding human sources have occurred repeatedly in the past. This report calls this the "recurring omissions" problem.

i. Misunderstanding Concepts

154. (U) NSIRA detected several factors that heighten the risk that regions will omit information material to the warrant application. Indeed, some duty of candour breaches seem to be explained by these factors[189].

155. (U) NSIRA was told that police learn how to piece together a narrative that "shows their work", and police informant handlers also are generally familiar with credibility and candour issues.[190] CSIS is not culturally attuned to this same standard,[191] despite the importance of the legal expectations it must meet. Indeed, CSIS officers, when writing intelligence reports, are trained to dissociate the substance of the intelligence from its provenance, in order to allow the resulting reporting to be disseminated to clients in government without permitting readers to infer the identity of sources.

156. (U) Indeed, there seems to be a disconnect between CSIS's traditional understanding of reliability for intelligence purposes, and the broader concept of credibility for legal purposes. Intelligence reliability is based on the source's track record as corroborated by other sources of information. Credibility, however, may depend on more information about the sources themselves, including their personal conduct and disposition. CSIS source handlers may, however, be inclined culturally to invest [description of relationship between source handler and source]

187 Interview(s).
188 Interview(s).
189 Interview(s).
190 Interview(s).
191 Interview(s).

[description of relationship between source handler and source][192] Moreover, NSIRA heard repeatedly that CSIS officers involved in the early stages of warrant preparation do not clearly understand the legal expectations associated with the duty of candour.[193]

157. (U) For these reasons, it has sometimes not occurred to these officers that conduct exhibited by the source – [example of source conduct] – may constitute material information important to a court in assessing the credibility of that source. CSIS may have long ago noted these issues, but nonetheless concluded that the source's reporting was generally accurate. Thereafter, officers may not realize that it is vital to put all such context before the Court. Officers may also misunderstand the implications of source shortcomings for the Court, fearing that their sources' information will be discounted because of personal shortcomings. In fact, the Court has understood that a source's moral shortcomings alone do not mean that the source cannot be believed; judges do not assume that sources in national security investigations will always be upstanding citizens, any more than they do in police organized crime investigations. This was recently reiterated by the Court, noting that *"the fact that human sources live what some would consider unsavoury lives is something to be expected when assessing human source information provided in the context of a CSIS Act warrant application".* [194]

158. (~~S~~) Under the current CSIS procedure on Human Source [name of procedure] every CSIS human source is assigned a [redacted] a brief and standardized description of [redacted][195] [redacted]

[Discussion of human source issues, including reliability and credibility] [redacted]

159. (U) The role of a judge in issuing a warrant is different. The judge must independently conclude that the information before them is reliable. In conducting this independent assessment, the judge must have all of the information they need to be satisfied that the source of the information is reliable and credible, even if CSIS believes that the information is accurate. The Federal Court recently noted that:

> *"Judges of this Court expect a Human Source Précis to bring to their attention all information known to the Service that might be relevant to the Court's assessment of the credibility or reliability of a human source. The Service must provide the Federal Court with a relevant and full picture concerning the credibility and reliability of a human source. This Human Source Précis must be relevant, full and complete if the Service is to comply with the duty of candour. The Service employee must not pull punches, conceal information, or convey half-truths, nor may he or she bring false or misleading information to the Court."*[196]

160. (U) To this end, CSIS's own assessment of a source's reliability may be relevant but it is not for the Court to take it on faith. The best analogy presented to NSIRA was this: the affidavit must "show CSIS's work" just as a math student shows the full calculation in computing an

---

192 Interview(s).
193 Interview(s).
194 2020 FC 1190 at para 163
195 Human Source [redacted] CSIS affidavit of [redacted] at para 18-22.
196 2020 FC 1190 at Par. 152

answer through long division. That is, the affidavit must contain the full range of considerations relevant to a source's credibility, and then explain why CSIS considers the source's information reliable. The judge can then make their own assessment, and not simply depend on CSIS's pre-existing conclusion.[197] Asserting that conclusion without "showing the work" and articulating the range of considerations tied to credibility amounts to a failure to be candid, particularly when CSIS has concluded that a source is reliable despite certain factors that, on their own, could give rise to doubts about the source's credibility. NSIRA believes this analogy to be a helpful one so long as "showing CSIS's work" includes the full range of information material to the issuance of the warrant, a point to which we return below.

161. (U) In summary, to avoid "recurring omissions" before the Court, CSIS must internalize a clearer understanding of the Court's role. This is particularly crucial amongst those involved in the preparation of warrants,[198] including source handlers compiling the initial information.[199]

ii. Information Management Struggles

162. ~~(S)~~ Even if CSIS officers were fully conscious of the scope of the concept of candour to the Court, the way in which CSIS manages its information would likely still give rise to recurring omissions. In its interviews, NSIRA heard that CSIS's management of information related to human sources creates problems. [Discussion of IM issues] [redacted] [Discussion of IM issues] [redacted][200] [redacted][201] [redacted][202]

163. ~~(S)~~ Information is often situated in the (changing and variable) institutional memory of source handlers. [Discussion of IM issues] [redacted][203] Any institutional knowledge not archived properly is lost, as Intelligence Officers (IOs) are rotated regularly under CSIS's human resources model.[204]

164. (~~S~~) Since source-related information [discussion of IM issues] [redacted] the review process can be laborious. When connected to the first factor noted above – a limited understanding by CSIS officers of legal materiality – mistakes are inevitable. Moreover, as operational reports written by handlers are sent through a hierarchal chain of approval, there is no method of tracking any changes made by supervisors to the handler's report, making it difficult to identify the origin of a problem should it arise.[205]

---

197 Interview(s), HSOS Briefing 2021 03 19.
198 Interview(s).
199 Interview(s).
200 Interview(s).
201 Interview(s).
202 [redacted]
203 Interview(s). [redacted]
204 Interview(s).
205 This is one of the gaps that is supposed to be rectified through the new [redacted] (discussed at Para 167 below). NSIRA Preliminary Briefings, September 18, 2020, [redacted]

iii. Fixing the Recurring Omissions Problem

165. (U) CSIS and NSLAG are alive to these problems. They have conducted more training on the need for adequate documentation in order to fulfill the duty of candour obligations to the Court.[206] Justice counsel have more access now than in the past to source materials.[207] Indeed, in the short term, in some cases, they have responded to the recurring omissions problem by involving warrant counsel directly in the review of source files.[208] Counsel auditing of source files is, however, resource intensive and arguably displaces a responsibility for source information preparation that properly lies with CSIS itself. It is the affiant, working with the regions, who should guarantee and be answerable for the accuracy of the source information, not counsel.[209]

166. (~~S~~) More generally, CSIS should ensure that source handlers are assiduous in documenting information going to credibility, no matter how seemingly unimportant.[210] The lack of adequate documentation was a key finding in the Rosenberg report, an independent review commissioned following a breach of the duty of candour to the court.[211] In response to it, CSIS set up Project [Name]. Its main objective was to encourage better documentation of the full picture of intelligence and operational activity with the goal of improving operational effectiveness.[212] One identified quick win now associated with [Name] was the regional roll out of [discussion of an information gathering tool] [redacted].[213] NSIRA was advised that this approach is being prioritized for sources whose information supports active warrants.[214]

167. (~~S~~) NSIRA heard, however, that completing [information gathering tool] is a considerable task, requiring a comprehensive and thorough review [requirements of the information gathering tool] [redacted].[215] Furthermore, NSIRA heard there is a certain level of frustration by source handlers at the implementation of this stand-alone requirement rather than building on preexisting [category of] documents, [examples of preexisting documents] [redacted]

168. (~~S~~) Indeed, CSIS acknowledges that it designed [information gathering tool] to be a temporary tool to address and mitigate the larger recurring omissions problem. One of the long-term goals of Project [Name] is to develop a system [objectives of the system] [redacted].[216] It is unclear if this system will be stand-alone, integrated into preexisting systems, or developed as part of a planned [Name] [redacted], designed to consolidate all the administrative processes and workflows required to manage a case and document its progression.[217] The [Name] is due to be partially

---

206 Interview(s).
This was one of the initiatives of project [Name]
207 Interview(s).
Affiant Unit Briefing April 12, 2021.
208 The Warrant Life Cycle -Affiant Unit Briefing December 4, 2020.
209 Interview(s).
210 Interview(s).
211 M. Rosenberg "Independent Review: Duty of Candour at CSIS", 2020 03 03, slide 11.
212 [Name] Presentation to NSIRA 2020 09.
213 Ibid, slide 12
The [tool] was initially developed by [Name] Branch. Ref: CSIS Factual Accuracy Check, December 22, 2021.
214 Interview(s)., Affiant Unit Briefing February 22, 2021
215 Interview(s).; HSOS Briefing 2021 03 19
216 [redacted] deck reference.
217 NSIRA Preliminary Briefings, September 18, 2020, [redacted]

implemented [timeline] while the proposed [Name] human source information system appeared to be aspirational and only at the early stages of identifying a possible solution.[218] This is unfortunate, as the [info.tool] represents a "band-aid" solution to issues that, in the long run, would be better addressed by deeper improvements to the management of human source information.

169. ~~(S)~~ Even setting aside longer-term considerations, a [info. gathering tool] process is not a panacea. For one thing, the [info. gathering tool] is only as good as the person completing it.[219] Until recently, there was no formal [info. tool] training for source handlers. More than a year after it was implemented, CSIS's Learning and Development Branch was unaware of the info gathering tool.[220] Furthermore, it should be possible to audit the responses provided in the [info. gathering tool] In the past, prior to the creation of the Affiant Unit (AU), the facting was formally reviewed by the [name of branch and positions conducting review] [221] Only [postion] had access to the full range of human source information, however, as verification was considered a "side of desk" task. Now, the AU has access to the human source files and NSIRA was told it reviews the original documents referenced in the [info. gathering tool] as well as running queries through human source and operational databases and consulting with the source handler.[222] To do this properly, however, the AU itself will need to be resourced and encouraged to audit the information prepared by the regions. This report discusses the question of the AU's sustainability below.

170. (U) Finally, several of the interviewees noted that the reformed process is revealing a number of "legacy problems" with CSIS human sources; that is to say, additional duty of candour issues are coming to light as a result of CSIS's more stringent review of human source files when preparing for warrants. This is indeed a regrettable consequence of CSIS's former lax practices. For the next few years, therefore, the Federal Court can expect to receive further duty of candour submissions. For its part, NSIRA will need to distinguish between those duty of candour issues rooted in past practices and those that have emerged despite the recent changes.

171. **Finding no. 16: NSIRA finds that CSIS has struggled to ensure that all information material to the credibility of sources is properly contained in warrant applications. This "recurring omissions" problem stems from a misunderstanding of the Federal Court's role in assessing the credibility of sources and from the presence of multiple, siloed information management systems. CSIS has undertaken reforms, but work remains to implement long-term sustainable solutions.**

---

218 HSOS Briefing 2021 03 19.

219 Interview(s).
J. Poirier Briefing Transcript, April 7, 2021, pg. 37.

220 Briefing with CSIS L&D, July 23, 2021.
NSIRA has been informed that CSIS has recently incorporated the [info tool] into its [Name] training. CSIS Factual Accuracy Check, December 22, 2021.

221 Lean Chief Review Final, Change to Chief Review, 2019 08 22

222 Interview(s). We were told that prior to the AU, HQ desks did not have access to [certain information] required to conduct full searches in the database. The AU does, although we were also told that obtaining permission to query the relevant databases requires multiple levels of approval that contributes to delays. Affiants, we heard, should have more autonomous powers to approve steps necessary to perform the necessary functions of the AU. Interview(s).

Recommendation no. 10: To address the seeming inevitability of "recurring omissions", NSIRA recommends that CSIS prioritize the development of [an improved] system for human source information management. CSIS should also continue initiatives meant to ensure that source handlers are assiduous in documenting and then reporting in source précis information going to credibility. Even with these reforms, the Affiant Unit should adopt procedures for verifying the information prepared by the regions.

c. The Affiant Unit

172. (U) As noted above, the individual most responsible for the final product is the affiant, whose sworn affidavit supports the warrant application and supplies the factual basis for concluding the legal requirements for the issuance of a warrant have been met.[223] Yet while NSIRA's interlocutors agreed that affiants are ultimately responsible for the affidavit, NSIRA notes that they have not been given a status and authority commensurate with this obligation.[224]

i. The Traditional Approach

173. (U) Pre-2019, CSIS recruited affiants in security intelligence investigations on an *ad hoc* basis in support of a particular warrant application. There was no such thing as a professional affiant. The result was considerable unevenness in the caliber and skill-set of affiants.[225] The employees assigned as affiants were, NSIRA was told, sometimes not the best possible candidate, but rather a person with down-time, surplus to immediate operational needs, and not necessarily experienced in the affidavit process.[226] The seeming casualness of affiant selection surprised NSIRA; the affiant is effectively CSIS's spokesperson to the Federal Court, which alone can authorize invasive investigative techniques. Ensuring a roster of excellent affiants should have been regarded as "mission critical" to CSIS.[227]

ii. The Current Approach

174. (U) In 2017, in response to the Segal report recommendations (see Annex A), the Affidavit Working Group (AWG) at CSIS recommended the creation of an Affiant Unit of *"experienced Intelligence Officers who would be dedicated full-time to the role of representing the Service in court"*.[228] The objective of this new unit was the creation of an actual centre of affiant expertise. The AWG recommended that affiants be employed at Level 10 (typically a senior manager) in the CSIS employment hierarchy *"indicating the seniority and importance vested in the role",*

---

223 Interview(s).
224 Interview(s).
225 Interview(s).
226 Interview(s).
227 Interview(s).
228 Briefing Note from Affidavit Working Group to the ADO, "Creation of a CSIS Warrant Section and the Professionalization of the S.21 Process", 2017-06-30, [redacted]
In determining the requisite number the Project Manager disregarded the 2018/2019 numbers which were "considered atypical given the various challenges with the Federal Court" and calculated that averages from 2014 to 2017.

with ongoing training and professional development being key components to the unit's success.[229] The AWG also proposed a process and structure for the development of the unit.

175. (U) CSIS ultimately created the Affiant Unit (AU) in 2019, after an order from the Director and during the Federal Court 2020 FC 616 matter.[230] NSIRA was repeatedly told that the resources allocated to the unit were based on estimates by the project management team in 2019.[231] The CSIS "End of Project Summary - Establishment of the Affiant Unit" identified the need for an AU structure that included "[number] Affiants" in order to accommodate past averages of [number] section 12 warrant applications annually.[232] For reasons that are not clear, the final approved structure cut the number of affiants in half, to [num.] The final structure therefore comprised [description of internal structure][233] The mandate of the AU was later expanded to include warrant applications for section 16 investigations by adding [number] although this affiant is managed out of the [Name] Unit and the Affiant Unit.[234] This report discuss the implications of how the AU has been staffed below.

iii. The Advantages of an Affiant Unit

176. (U) Professionalizing affiant work involves trade-offs. For instance, dedicated affiants are better placed to develop and implement consistent processes and standards regarding warrant preparation, but will often have less mastery of the operational details than an affiant chosen from an operational desk, thereby obliging the affiant to spend considerable time familiarizing themselves with the details of each application.[235] Still, our interviewees were consistently of the view that despite the trade-offs, the dedicated affiants and the AU itself represented a significant improvement over the prior *ad hoc* approach,[236] and noted that the new dedicated affiants have been well received by the Court. Indeed, NSIRA is of the view that a well-staffed AU should constitute a body of expertise on warrant preparation within CSIS. Robust vetting by the AU could also replace many of the seemingly *pro forma* steps in the current warrant process that contribute little of substance.

177. (U) Justice counsel reported having effective working relationships with the affiants, whom they considered to be knowledgeable and professional.[237] For reasons discussed below, however, some counsel were concerned that the affiants were at risk of burn out, and raised concerns regarding the sustainability of the AU.[238]

---

229 Ibid
230 Affiant Unit Briefing, September 17, 2020.
231 Affiant Unit Briefing February 22, 2021.
232 End of Project Summary- Establishment of the Affiant Unit, 2019-12-24, File # 100-72-5
233 Ibid
234 CSIS Factual Accuracy Check, December 2021.
235 Interview(s).
236 Interview(s).
The previous approach to assignment of affiants was described in internal CSIS documents as "*Service officers who are called upon to be affiants already have a "day job" as case officers or desk heads; the affiant role is one that they are parachuted into, often unexpectedly or in an ad hoc manner. Affiants are sometimes chosen largely according to availability, with horse-trading taking place in different corners of the Service to free up an officer",* Briefing Note to the ADO from the Affidavit Working Group, Creation of a "CSIS Warrant Section" and the Professionalization of the S.21 Process, June 30, 2017,
J. Poirier Briefing Transcript (April 7, 2021) [Top Secret] p. 40, line 6.
237 Interview(s).
238 Interview(s).

178. (U) With regard to the regions, we heard that some affiants, on their own initiative, regularly communicate with regional partners, potentially creating links that could forestall future duty of candour problems.[239] Indeed, NSIRA heard that investigators and their managers welcomed the AU as the path to obtaining warrants.[240] NSIRA was told that AU/regions communication should be a standard practice given the current communication silos existing between headquarters and the regional units responsible for executing warrants.[241] NSIRA agrees that affiants should consistently consult with the regions to understand how the proposed warrants will be executed and to understand generally what is working and what is not.[242] NSIRA notes that experienced affiants could serve as critical sources of institutional knowledge while field officers in the region cycle in and out.[243] Moreover, this interaction between affiant and regions should help counsel anticipate any possible candour matters that could arise were the Court not apprised of potentially controversial means of executing warrant powers.[244]

iv. Challenges to Affiant Unit Sustainability

179. (U) As explored above, CSIS's establishment of the AU is a critical development. It is thus all the more concerning that the AU's sustainability is in question, and indeed NSIRA heard that the unit could currently be described as in a state of crisis. CSIS has not supported the unit with resources commensurate with the importance of this unit in fulfilling CSIS's mission.[245] Indeed, there may now be less support to affiants operating from the AU than existed under the prior regime of *ad hoc* affiants supported by other units in CSIS.[246]

180. ~~(S)~~ The AU faces several overlapping challenges. Over the course of NSIRA's review, AU staffing was in considerable flux, with personnel cycling through affiant, analyst and management posts. Indeed, by summer 2021, the key role of analysts – usually charged with compiling material from the region and the initial drafting of the affidavit and human source précis – was filled by [number] temporary analyst.[247] Of the [number] new affiants hired by the AU during our review, [number] had left by the end of it.[248] Meanwhile, the remaining affiants were cycling through a vacancy as [position] (of the AU). In the result, it would appear there were only [number] people able to act as affiants for [type of warrant] and [number] [type of warrant] summer 2021.

181. (U) NSIRA heard that joining the AU is an unattractive career choice, because CSIS's human resources policies do not support the stated objective of professionalizing the warrant process. Affiants, much like many at CSIS who are not Intelligence Officers, do not gain the operational experience that is traditionally tied to status and advancement.[249]

182. (U) At the time of writing, the AU was relying on "surge capacity" by drafting analysts available temporarily from other units of CSIS.[250] NSIRA heard that these temporary analysts lack

---

239 Interview(s). Affiant Unit Briefing December 4, 2020, February 22, 2021.
240 Interview(s).
241 Interview(s).
242 Interview(s).
243 Interview(s).
244 Interview(s).
245 Interview(s).
246 Interview(s).
247 Interview(s).
248 Interview(s).
249 Interview(s).
250 Affiant Unit Briefing December 4, 2020, February 22, 2021.

warrant experience.[251] They thus need to be trained by the affiants, only to depart and be replaced. This has added to the burden on affiants, some of whom now complete the drafting process once led by analysts.[252] This also contributes to the workload of NSLAG counsel, who must help fix draft products.[253]

183. (U) Moreover, the benefits of the AU are currently in jeopardy because of governance and training deficiencies. The AU did not inherit an existing infrastructure or suite of policies and professional standards. The affiants at the time of our review were experienced CSIS officers who often had some prior affiant experience. Those affiants who have been in the AU for a length of time have deepened their expertise through learning on the job. However, none of the affiants or supporting analysts received formal training on their roles.[254] CSIS has not yet put in place a training system to ensure continuity of a standard base of knowledge and skills in the AU. Even if it did, the AU is already under-resourced, fueling turnover, and NSIRA doubts whether the AU has the time and capacity to step back from the day-to-day work in order to build expertise and human capital. For instance, weekly meetings with NSLAG counsel have often been impossible due to time constraints, making it harder for the AU to stay apprised of legal issues.[255]

184. ~~(S)~~ It is clear that the AU cannot continue to operate in its present manner, and that the risk of burnout for the remaining staff is real. As this review progressed, NSIRA became increasingly concerned that the AU [redacted] [is in a state of crisis] [redacted]. The apparent neglect of the AU's human resources needs is alarming: the AU is not only a key element of CSIS's response to its recurring candour problems, but it is also operationally vital. Without a functional AU able to produce accurate and compelling warrant applications in a timely manner, [redacted] [discussion of how CSIS collection activities are affected] [redacted].

v. Improving and rebuilding

185. (U) It is clear that the AU needs to be stabilized and expanded by an immediate infusion of new personnel. NSIRA asked how an expanded AU could function, and in response received remarkably consistent responses:

- "Affiant Teams": NSIRA heard that each affiant should be supported by [redacted] [discussion of number of analysts, administrative assistants and paralegals required] [redacted][258] – forming an expert team. Teams should specialize in counterintelligence or counterterrorism,[259] and should be managed so not everyone leaves as the same time.[260] Likewise, files should be managed so that inexperienced affiants and affiant teams are not paired with inexperienced lawyers.[261]

---

251 Interview(s).
252 Interview(s).
253 Interview(s).
254 Interview(s) Affiants have access to a basic Affiant Training deck [redacted] however this deck [redacted] [NSIRA critique of training contents] [redacted]
255 Interview(s).
256 Interview(s).
257 Interview(s).
258 Interview(s).
259 Interview(s).
260 Interview(s).
261 Interview(s).

- Workload expectations: NSIRA heard that a professional affiant should be able to manage [numbers] affidavits annually, although others emphasized that [numbers] was feasible.[262] The lower estimate is closer to CSIS's own calculation that "given that each application takes approximately [timeline] one affiant could process [number] applications per year."[263] At this rate, the present roster [number] should be able to generate [number] warrant applications annually. This assumes that affiants are adequately supported, however, which was not the case as of summer 2021. [numbers] warrants annually would seem inadequate given CSIS's investigative needs. CSIS will not be able to acquire more warrants without either sacrificing the quality of its applications – and risking new candour problems – or expanding the AU.[264] Moreover, as discussed below, [number] warrants is fewer than the number of warrants that NSLAG is now equipped to support.

186. (U) Building bigger, skilled and stable affiant teams will require new people willing to join the AU and stay for a reasonable length of time. NSIRA believes achieving this objective requires two sets of reforms: first, changes to career development within the AU; and second, greater institutional commitment.

187. (U) Without human resources reform and firm prioritization of the AU, NSIRA doubts CSIS will be able to recruit and retain a talented cadre prepared to specialize as affiants and analysts. The ideal affiant, NSIRA was told, was a great analyst and writer, with advanced research skills and robust institutional knowledge about how CSIS operates and how, especially, source information is retained. They must, in addition, be comfortable in court and have an understanding of applicable law.[265] Some affiants have handled sources, while others have not. Source handling experience was not regarded as essential by at least some interviewees,[266] but it was felt that the affiant needed people skills and an ability to manage the affidavit process and relationships with the regions.[267] A successful affiant should have gravitas and an ability to persuade other partners in the warrant process.[268] Moreover, once these people are recruited, like any expert, affiants and analysts need to acquire institutional knowledge – and the AU will need to resist the level of turnover we were told is endemic in CSIS.

188. (U) NSIRA heard that retaining talent will require attention to several problems. Unlike with at least some police forces,[269] CSIS assigns little prestige to this career path. Indeed, CSIS human resource policies risk orphaning affiants in career limbo, with no natural career progression and advancement path given that time in the Affiant Unit is not time spent gaining front-line operational experience.[270] Specifically, affiants are classified as a "level 9" in the CSIS human resources hierarchy, but only temporarily (if not already level 9). If advanced from level 8 to be an affiant, they return to level 8 if they leave – or must compete for a permanent level 9 elsewhere in CSIS.[271] Despite the considerable pressures on affiants to manage a complicated warrant process and represent CSIS credibly before the Federal Court, affiant work is reportedly not countenanced as meeting prerequisites for promotion into management.[272] Being

---

262 Interview(s).
263 End of Project Summary- Establishment of the Affiant Unit, 2019-12-24,
264 Interview(s).
265 Interview(s).
266 Interview(s).
267 Interview(s).
268 Interview(s).
269 Interview(s).
270 Interview(s).
271 Interview(s). A level 9 at CSIS equates to an EC-6 in core government. Since some of these positions are filled on a temporary basis, the initial L8 position from which the individual is transferring from remains "on hold" thereby making it less desirable for management to release the person, as they are not able to backfill the position.
272 Interview(s).

an affiant is, in other words, not a clear career progression so much as a career diversion.

189. (U) CSIS has also struggled to resource permanent analysts for the AU. Analysts, much like other non-intelligence officer (non-IO) employees at CSIS, are left with so few career progression options that they often feel like second-class citizens within the organization.[273] In order to attract talented analysts, there must be incentives allowing for progression within the non-IO stream, including the AU.[274]

190. (~~S~~) As this discussion underscores, the AU needs more resources, especially in the form of analysts and affiants. However, the AU is left to compete for resources as just another unit under the broad umbrella of the [Name] Branch [Name].[275] NSIRA heard that the AU's functions in preparing legally robust warrant applications are not a natural subset of [Name and function of Branch] and that the AU is not well situated in the present structure.[276] This governance anomaly may explain a number of administrative hurdles and human resource and sustainability issues. A new governance structure, with reporting mechanisms consistent with the importance of the function needs to be instituted.

191. (U) A new Affiant Branch needs to be created and situated in CSIS's organizational hierarchy reporting directly to the CSIS Director.[277] This would be consistent with the Director's direct accountability as provided by CSIS Act and signal the AU's importance to CSIS's ongoing success and presumably ease the risk of neglect. This change would coincide with the elimination of the often-unnecessary hierarchy of approvals that exist as a result of the AU's current status as part of [Name] branch. This change may also respond to another observation: that priorities not directly visible to the Director sometimes stall lower in the CSIS hierarchy,[278] and that reform also stalls among managers who do not have a clear incentive to change.[279]

192. (U) In sum, NSIRA believes that CSIS's success in overcoming its long-standing difficulties with the warrant process will depend on a robust Affiant Unit. In our future reviews of the warrant process, NSIRA will be attentive to CSIS's progress in sustaining a robust AU.

193. **Finding no. 17: NSIRA finds that the Affiant Unit (AU) constitutes a vital and laudable reform within CSIS. However, the AU is currently at risk of collapse. CSIS has not supported the unit with resources commensurate with the importance of this unit in fulfilling CSIS's mission. The benefits of the AU are currently in jeopardy because of governance, human resource, and training deficiencies.**

---

273 Comments on Yes, Leadership does Matter! The Source, July 2021.
This culture is not unique to CSIS alone. It was noted over twenty years ago in an analysis by the US sub-committee on Foreign Relations Making Intelligence smarter: the Future of US Intelligence The sub-committee noted, "The best way to ensure high-quality analysis is to bring in high quality analysts into the process. Analysis would be improved by increasing the flow of talented people into the Intelligence community for outside the Government. Greater provision should be made for lateral and mid-career entry of such analysts…".Ref- making intelligence smarter.

274 As noted, IOs joining the AU are given temporary promotions for the duration of their time with the AU, affiants are not promoted, and they are transferred at level.
End of Project Summary- Establishment of the Affiant Unit, 2019-12-24, File #

275 Interview(s).
The Director General of is responsible for each of which is further divided along many operational lines.

276 Interview(s).

277 Interview(s).1; see Annex C showing the comparison between the current and the recommended structures

278 Interview(s).

279 Interview(s).

194. **Finding no. 18: NSIRA finds that the Affiant Unit's placement in the [Name] branch is not commensurate with its functions and importance. This governance anomaly most likely contributes to administrative hurdles and resource challenges faced by the AU.**

195. **Finding no. 19: NSIRA finds that without a functional AU able to produce timely and accurate warrant applications, CSIS puts at risk access to warrants and the information collected under them.**

In view of the above findings with respect to the AU, NSIRA recommends that:

Recommendation no. 11: CSIS recognize the importance of the Affiant Unit by assigning affiants and analysts an employment classification congruent with their responsibilities.

Recommendation no. 12: CSIS create an Affiant Branch reporting directly to the CSIS Director.

Recommendation no. 13: CSIS urgently resource the Affiant Unit to meet its responsibilities and ensure its sustainability. In deciding the size of the AU, CSIS should assess how many warrants an affiant team might reasonably complete every year.

Recommendation no. 14: CSIS, in consultation with Justice, develop a comprehensive training course for all affiants and analysts, codifying best practices and methods for members of the AU.

d. NSLAG Warrants Counsel

196. (U) Warrant counsel have several key roles anticipated in the CSIS warrant application process, and are intimately implicated in securing adherence to the duty of candour in warrant applications. As noted, the duty of utmost candour in warrant proceedings is a professional obligation that rules of professional conduct impose on lawyers.[280] Crown counsel in police warrant cases have a redoubled incentive to test warrant applications – no Crown wishes to be the lawyer on a warrant that subsequently fails on *ex post facto* challenge in a criminal proceeding, jeopardizing a prosecution.[281] While NSLAG counsel face different pressures, duty of candour failures still risk professional reputations, especially given the vigorous displeasure expressed by Federal Court judges in their judgments.

197. (U) It seems clear that, as a result of 2020 FC 616, NSLAG has weathered a difficult period. Counsel reasonably see themselves as both personally in the cross-hairs of the court's discontent and dependent on CSIS managing its responsibilities in the warrant process in a way attentive to its legal obligations.[282] From the counsel's perspective, the process feels like a high risk enterprise, over which hangs a "sword of Damocles".[283] For its part, as noted, CSIS

280 See, e.g., Federation of Law Societies, Model Code of Professional Responsibility, Rule 5.1-1.
281 Interview(s).
282 Interview(s).
283 Interview(s).

operational employees may regard Justice as inaccessible and unhelpful. Lawyers vary in their style and manner of operating, with no consistency.[284]

198. (U) Some lawyers have responded to duty of candour failures by becoming more meticulously involved, in a way described by some CSIS observers as intrusive, micro-managing matters that CSIS feels it should handle.[285] It is apparent that tensions have increased in the last several years between Justice and CSIS, shaped by these perceptions each has of the other. This tension was especially acute, NSIRA was told, at the more senior levels, with some noting that little had improved by the time of our interviews.[286] NSIRA also heard about the need to correct this situation by building mutual trust.[287] This section focuses on the structural sources of those tensions and the prospects of restoring confidence.

199. (~~S~~) First, CSIS interviewees urged that CSIS needed access to more lawyers,[288] sometimes seeing lawyers as the bottleneck in the warrants process.[289] Other interviewees contested this view.[290] These different views may reflect change over time. It is clear that during a recent period, NSLAG had too few available warrant counsel.[291] That situation appears now to be evolving, as new lawyers are recruited by NSLAG. NSIRA agrees, however, with the principle that NSLAG should be staffed to ensure that CSIS's operations are not stalled due to the non-availability of warrants counsel.

200. (U) At present, a General Counsel is the strategic lead for warrants and Federal Court matters.[292] In addition, the Senior Counsel warrant coordinator oversees the warrant applications led by NSLAG warrant counsel. The senior counsel warrant coordinator would ideally not manage their own files, and instead would maintain comprehensive visibility on the warrant practice, while assisting and mentoring new warrant counsel. These positions must also bridge the warrant and advisory side of NSLAG, ensuring that emerging legal issues are shared.[293]

201. (U) The number of actual warrant counsel will affect how many warrants CSIS might seek at the Federal Court. NSIRA asked for views on a metric for determining the ideal number of counsel. Whereas an experienced warrant counsel might once have transacted [number] warrants annually, the scope and scale of applications is now such that the maximum number is [range] Given this number, and with a roster of [number] experienced warrant counsel (and several more junior) available by the second half of 2021,[294] the maximum number of warrants NSLAG might support annually may be in the 30-60 range. Notably, this number is several multiples above the number of affidavits the AU is presently equipped to manage, assuming the calculations provided above.[295] These calculations seem to affirm the views that resourcing issues at the AU now constitute the critical bottleneck, whatever may have been the case in the past.

---

284 Interview(s).
285 Interview(s).
286 Interview(s).
287 Interview(s).
288 Interview(s).
289 Interview(s).
290 Interview(s).
291 Interview(s).
292 Department of Justice, Warrant Process Briefing, December 18, 2020, Transcript Pg. 8.
293 Interview(s).
294 Interview(s).
295 CSIS RFI 3, Question 5, Number of Warrants, 2021 07 14.
In 2017, CSIS applied for 28 warrants (including section 12 and 16) compared with 12 applications in 2020.

202. (U) NSIRA also heard views about the importance of mentoring of new warrant counsel by experienced warrant counsel, and how NSLAG must make this a priority.[296] This includes the need for junior lawyers to be trained on matters pertaining to CSIS tradecraft and technology.[297]

203. (U) NSLAG recruitment also emerged as an issue in NSIRA's discussions. NSLAG is regarded by other components of Justice as too close to its client and concerned with maintaining an ongoing relationship with the client, a characterization regarded as unfair by the interviewees who addressed it.[298] Morale in NSLAG was badly affected by the 2020 FC 616 saga.[299] NSLAG's practice area is also, from the perspective of many lawyers, obscure and narrow, and not necessarily perceived as part of a Justice lawyer's ideal career path. Employment at NSLAG requires enhanced security clearance, including a polygraph. The clearance process may be lengthy, and prospective employees may lose interest in the interim.[300] These factors together contribute to NSLAG recruitment challenges.

204. (U) NSIRA notes that the range of professional backgrounds among counsel seems to be increasing, and more NSLAG warrant counsel have prior experience with warrants. NSIRA was told NSLAG has been encouraged to hone its public law expertise, as well as recruit lawyers with criminal law experience.[301] NSIRA welcomes these developments and will consider NSLAG's evolution in future reviews.

Recommendation no. 15: NSIRA recommends that NSLAG be staffed by a complement of counsel and support personnel sufficient to ensure that CSIS operations are not impeded by resource limitations at NSLAG.

e. Revamping the Independent Challenge Function

205. (U) The warrant application process is buttressed by a review of the near-final affidavit by an "independent counsel" (IC) – in practice, a lawyer drawn from the National Security Group (NSG) of the Department of Justice. "Independent" in this context means, therefore, at arm's length from CSIS and NSLAG and otherwise not implicated in the warrant process.

i. The Imperfect Independent Counsel Model

206. (U) The IC position was created in 1988 following the 1987 "Atwal" matter in which extensive errors were made in a CSIS warrant application (Annex A). In its 1986-1987 Annual Report, SIRC noted that the Solicitor General in consultation with CSIS should consider whether there ought to be a devil's advocate position at some stage of the warrant process to argue the case against the warrant.[302] The position of the devil's advocate was described as an official appointed to ensure that all aspects of a matter are fully considered.[303] The following year, the "devil's advocate" position had been established, yet, SIRC noted that, *"at present the devil's*

296 Interview(s).
297 Interview(s).
298 Interview(s).
299 Interview(s).
300 Interview(s).
301 Interview(s).
302 SIRC, annual Report 1986-1987, pg. 9
303 Ibid

advocate does no more than ensure that the information CSIS intends to cite in a warrant application is accurate. We had in mind, rather, someone who would challenge the need for a warrant at all - someone to make the case that the proposed target (who does not of course even know a warrant is being sought) might make."[304]

207. (U) Ultimately, very little has changed. NSIRA was informed that the primary goal of the IC is to "ensure that, as much as possible, factual mistakes don't make their way into the material that is submitted to the Court".[305] Scrutiny of the warrant is done through reviewing documents to ensure that factual assertions in the affidavit are accurately sourced.[306]

208. (U) The IC is charged with playing a fact-checking function, described as largely a form of checking the characterization of facts in the affidavit and source précis against the source material.[307] NSIRA was informed that NSLAG and CSIS were once more resistant to questioning by the IC. This situation has reportedly improved in the last several years, with counsel and CSIS described as now accepting of this querying.[308] In reality, however, changes proposed by the IC are usually very minor. Every once in a while, IC reported finding contradictions in the source material relevant to credibility issues, or treatment in the affidavit that were not justified.

209. (U) There will always remain inherent limits to the role of an IC coming at the end of the process. It cannot protect against all duty of candour shortcomings. Additionally, NSIRA noted a number of factors that have contributed to the inability of the IC to perform a robust challenge function:

- Lack of policy and training: short of a two-page document outlining the description of the IC function, there are currently no up to date internal policies, guidelines, or criteria governing the expectation or mandate associated with the IC role – much depends on the individual expertise of, and investment of effort by, the IC.[309] NSIRA was informed that typically new IC shadow senior IC counsel on their applications before being given their own. There is no official training program; counsel are given a binder of historical documents outlining the genesis of the IC role and where necessary may be given additional training on how the warrants process works.[310] Mentoring may therefore be inconsistent due to the absence of a standardized training program and clear descriptions of the required functions of the IC.

- Lack of knowledge: at NSG, counsel conduct their IC role as a supplement to their main legal work, involving among other things *Canada Evidence Act* s. 38 proceedings. By one estimate, IC work constitutes less than 5% of what NSG counsel do, and the NSG does not otherwise have any involvement in warrant-related activities.[311] The IC have little visibility on developments in the Federal Court, including on the specific CSIS warrants they have challenged. There is no formal debrief mechanism, no proactive sharing of classified reasons, and NSG counsel neither convene their own best practices/issue sharing sessions

---

304 SIRC, Annual Report 1988-1989, pg. 61-62

305 Briefing Transcript, Catheryne Beaudette, December 18, 2021, Page 8 at 17-20

306 Ibid pg. 11.
Noteworthy, the IC does not have access to full human source files.

307 The IC signs a certificate attesting that they are satisfied that the information in the human source precis and affidavit is a) contained in CSIS records; b) appears to be reliable; c) accurately reflected; d) presented in its proper context.
A [redacted] Review Checklist is provided to the IC, however, this list is outdated and does not reflect the issues of concern regarding Human Source information that have been of concern to the courts in the last several years.

308 Interview(s).

309 Step by Step Description of the Performance of the IC Function, Briefing Book, Tab B, December 18, 2021.

310 Briefing Transcript, Catheryne Beaudette, December 18, 2021, Page 50-51

311 Interview(s).

nor participate in NSLAG's sessions discussing emerging issues relevant to warrant practice.[312] Some IC noted that this lack of exposure to warrant-related activities results in a lack of knowledge needed to perform a more probing review or address broader issues beyond fact checking.[313] These knowledge constraints mean that it is extremely unlikely that the IC will be able to ask probing questions of the sort necessary to unearth the duty of candour issues stemming from possible issues on how a warrant might be executed – the second class of candour issues noted above. Meanwhile, counsel who may have this relevant experience, joining NSG from NSLAG, are required to wait a year before undertaking any IC functions. This means that often by the time they inherit a warrant file they are likely no longer current on recent CSIS practices.[314]

- Lack of access and time: the IC does not currently have timely access to the breadth of underlying information that would be required to play an authentic challenge role meaningfully. The IC does not receive important components of the warrant application in advance, including the source précis, and is often provided with very short deadlines for reviewing documents. While ICs have recently obtained some on-premise (CSIS) access to these other materials, this sort of advance review is uncommon.[315] The IC is not encouraged or provided with sufficient time to fully test the theory of the case presented in an application as a form of "red team" exercise. Nor can they be expected to counter the recurring omissions issue, discussed above. It is unlikely, therefore, that the IC is fully effective in addressing candour issues resulting from failure to disclose information material to credibility.

210. (U) The result has been an IC role that is often regarded as more clerical than substantive, designed to cite check rather than assertively peer review.[316] Indeed, the majority of interviewees involved in the warrants process regarded the IC as unhelpful as a form of quality control.[317] Recent changes in the CSIS warrant process indicate that the IC "challenge" is to be completed one day prior to the WRC and once the affidavit has already been circulated to WRC participants. This change is further reflective of the general view that the IC serves only to fact check or that nothing substantial will arise from the challenge that necessitates changes prior to the WRC.[318] Some interviewees doubted that the IC's role was necessary – a good, well-supported affiant should suffice to guarantee the facting.[319] NSIRA has commented above on how professionalized affiants are able to contribute to quality control.

211. (U) Still, NSIRA believes that the presence of an independent challenge in the system is necessary. NSIRA fears, however, that the current IC is largely a *pro forma* feature of the CSIS warrant process, giving the impression of a robust check and balance without accomplishing this objective.[320] NSIRA remains unpersuaded that a robust devil's advocate is best situated at Justice, drawing on lawyers from NSG. As noted above, while some individuals have a background involving warrants of various sorts, NSG lawyers are not, in their role, experts in warrants or necessarily knowledgeable about CSIS. Nor does NSG have any formal role in the

---

312 Interview(s).
313 Note this concern regarding lack of knowledge was also voiced by counsel interviewed as part of the Sims report, *please see Annex A.*
314 Briefing Transcript, Catheryne Beaudette, December 18, 2021, Page 49 at 8-11.
315 Interview(s).
316 Interview(s).
317 Interview(s).
318 Please see Annex B
319 Interview(s).
320 One such example is the attestation in the certificate that the information "is presented in its proper context", absent access and knowledge to the systems, operations and process, it may be impossible to make this affirmation.

warrant approval process. NSG would appear simply to be a convenient place to situate the IC, among lawyers who are security-cleared for very different functions. Put another way, a robust devil's advocate function has yet to be created, and there is no reason to prefer it be situated in another branch of Justice. As discussed next, NSIRA would propose the creation of this function in the third agency of government whose precise role is oversight of the CSIS warrant process: Public Safety.

ii. Reconceiving Public Safety's Oversight Role

212. (U) Public Safety Canada is the vessel through which the Minister exercises their oversight role, one intended by Parliament to be robust. The Minister's role in the warrants regime is enshrined in legislation. Section 21 of the *CSIS Act* mandates that an application for a warrant may only be filed "having obtained the Minister's approval".[321] The Minister's role on section 12 warrants therefore requires that the Minister is aware of the full implications of the application, including determining if the intrusive methods to be used are justified by the gravity of the threat to the security of Canada.[322]

213. (U) Yet, Public Safety has not had full visibility on the various aspects of the warrants application. There has traditionally been an information asymmetry favouring CSIS with whom the information resides.[323] This challenge was further exacerbated by capacity issues at Public Safety, including limited ability to access information and knowledge necessary to assess risk for the Minister.[324] The 2019 Ministerial Direction for Accountability (2019 MD) and the Framework for Cooperation between Public Safety and CSIS, sought to decrease the information asymmetry problems and increase ministerial oversight of CSIS.[325] Pursuant to section 8 (i) of the Framework, CSIS must update Public Safety on reviews conducted by NSIRA. NSIRA interprets this obligation to mean an ongoing commitment by CSIS to provide periodic updates on the progress of reforms to the warrant process including the implementation of the recommendations in this review which will inevitably affect warrant applications.[326]

214. (~~S~~) Functionally, Public Safety officials review all warrant applications with the support of legal counsel assigned to the department. Once the warrant application is received by Public Safety, officials will typically review the warrant for: clarity and logic; legal issues; candour issues; policy considerations; and additional considerations such as issues related to the impact on Canadians.[327] The Public Safety delegate will attend the WRC. Following the WRC, and once the warrant has been reviewed, Public Safety officials draft a briefing note summarizing the nature of the threat posed by the target of the warrant, along with a recommendation memorandum for the Minister's consideration.[328] If approved, Public Safety sends the application back to CSIS to be filed in Court.

---

321 Furthermore, section 7 (2) of the *CSIS Act* requires that the Deputy Minister be consulted before warrant applications.

322 NSIRA briefing with Public Safety Canada, July 16, 2021.
Briefing for NSIRA: Public Safety and Ministerial Accountability, slide 5.

323 Ibid (NSIRA briefing with Public Safety Canada, July 16, 2021).

324 Ibid

325 Ibid, also Ministerial Direction for Accountability, 2019.
Framework for Cooperation between Public Safety Canada and the Canadian Security Intelligence Service, 2020.

326 Ibid, Section 8 mandates the information sharing and collaboration between Public Safety and CSIS. Section 8 (i) requires that CSIS provide public safety with "Reviews conducted by the national security bodies involving CSIS's activities. Section 25 requires that these update be provided on a quarterly basis.

327 Ibid slide 6

328 Ibid

215. (U) Some Public Safety practices are of relatively recent vintage, prompted to some large degree by 2020 FC 616. NSIRA cautions, however, that Public Safety is not well positioned to perform a thorough challenge of the warrant application. First, asymmetrical access to information means that Public Safety does not review the ingredients comprising the warrant application, including the source file materials or even the source précis. It would not be realistic, in our view, to expect Public Safety to audit the full information trail leading to the warrant application – it will never be able to cure a "recurring omissions" problem. Again, NSIRA believes skilled affiants in the AU validating information received from the regions and performing peer reviews of each other's work product constitute the best means of verifying inclusion of the correct information.

216. (~~S~~) On the other hand, Public Safety should be positioned to solve systemic and governance issues giving rise to the second category of duty of candour issues noted in this review – those stemming from issues underlying the warrant and material to a judge's exercise of discretion. As noted by Justice Brown in reference to the failure of CSIS to flag high-risk human source operations, which were subsequently the subject of a warrant application before the Court: *"the responsibility for fully informed decision-making lies on every person participating in the decision".*[329] Situated at some distance from CSIS and warrant counsel, an adequately staffed and expert Public Safety vetting team should contemplate the blind spots from which those closer to the process may suffer. Indeed, NSIRA learned that Public Safety, even as presently constituted, at times raises such issues.[330] In this manner, Public Safety is in a much better position to anticipate lurking candour issues than is a lawyer at NSG, tasked with conducting an IC as a secondary function of their job. For this reason, NSIRA favours a new reform that would bolster Public Safety's vetting process, and would replace the NSG IC, all in service to the Minister's legislated oversight role.

217. (U) To this end, NSIRA favours a devil's advocate model that helps meet the Minister's own obligation to oversee the warrant process. That is, NSIRA recommends the creation of a role meeting the original vision proposed by SIRC in the report noted above: "someone who would challenge the need for a warrant at all - someone to make the case that the proposed target (who does not of course even know a warrant is being sought) might make". The counsel should be as assiduous as a defence lawyer would be, defending a client in a fully adversarial process. They should know, and know how, to ask questions about the information supporting the warrant, its planned execution, and any relevant surrounding context that might escape the attention of a lawyer less familiar with warrants or CSIS procedures and functions, or might be lost to tunnel vision among those closer to the application. In this manner, NSIRA suggests that this person, working with Public Safety's warrant vetting team, should be well-situated to anticipate the second category of candour issues discussed in the report.

218. (U) Right now, Public Safety is supported by its own Justice departmental service unit. NSIRA suggests that unit should be supplemented by a seconded counsel with practical warrant experience employed at the Public Prosecution Service of Canada, the private sector or elsewhere, independent from Justice management, and not otherwise involved in CSIS warrant applications. This counsel would be deployed for the specific purpose of supporting a Public Safety warrant vetting team in its challenge function. This challenge and review of the warrant conducted by the seconded counsel must be documented in a manner that is visible to the Minister when considering whether to approve the proposed warrant application. NSIRA cautions that the purpose is not to increase the number of steps or the length of time the application takes. Rather, abolishing the current IC model entirely in favour of a true devil's

329 2020 FC 1190.
330 Public Safety Briefing, 16 July 21

advocate conducted as part of ministerial oversight would thin the process in addition to reinforcing it with a built-in, thorough challenge function.

219. **Finding no. 20: NSIRA finds that the "independent counsel" (IC) role falls short of creating a thorough challenge function.**

Recommendation no. 16: NSIRA recommends that the function of the Independent Counsel as performed by NSG counsel at the Department of Justice be eliminated, in favour of a new challenge function, analogous to the role a defence lawyer would play were warrants subject to an adversarial process, situated at Public Safety and supported by the Public Safety vetting team, and performed by a knowledgeable lawyer from the Public Prosecution Service of Canada, the private sector, or elsewhere, who is independent from Justice management and not otherwise involved in CSIS warrant applications.

f. Submission to the Federal Court

220. (U) The final stage in the warrant process is the proceeding before the Federal Court. No warrant exists until authorized by the Federal Court. However, trust between the Federal Court, NSLAG and CSIS has clearly been strained by the long history of duty of candour failures.

221. (U) The Court is perceived by interviewees as more assertive now than in the past.[331] Some interviewees described doubts about the degree of control exercised by the Court,[332] sometimes seeing it as more akin to a review function and less like the classic judicial control exercised by a court in issuing (or not) warrants.[333] Others rejected any notion that Justice questioned the legitimacy of the Court's approach.[334] Still, the institutions implicated in the warrant process seem to have entered a cycle in which duty of candour failures have contributed to a climate of mistrust involving closer scrutiny and more searching judicial control,[335] which inevitably heightens anxiety at the CSIS level about operational implications and reputational risk. It has also been the source of some uneasiness at Justice.[336]

222. (U) Of particular note, interviewees told NSIRA that anticipating in advance the full range of considerations relevant to a judge in exercising their discretion is not easy, especially since judges reportedly focus on different concerns depending on the case before them. This creates a residual category of information that may have to be provided with the application.[337] CSIS and Justice reportedly now err on the side of being over inclusive.[338]

223. (U) Because of all of these factors, the warrant application process currently operates like a ratchet, as ever more detail is layered into the affidavit and supporting documents in an effort to anticipate and avoid a new duty of candour failure. There is some "cut and paste" possible for recurring issues, but this material must be tailored to each warrant, and then re-vetted through

331 Interview(s).
332 Interview(s).
333 Interview(s).
334 Interview(s).
335 Interview(s).
336 Interview(s).
337 Interview(s).
338 Interview(s).

the bureaucratic warrant approval process.[339] The resulting warrant applications become more lengthy, complex, and time-consuming to prepare.[340]

224. (U) Breaking this cycle, however, requires restored credibility through change at CSIS and Justice, not resistance. NSIRA believes that doing so requires an embrace of the recommendations made in this review. It also notes other ways in which CSIS and Justice could show a commitment to candour, possibly alleviating the workload involved in warrant applications. NSIRA noted one approach suggested by our interviewees: warrant applications would describe information that is excluded (because it is believed not to be material) in sufficient detail that a judge might ask for its disclosure should they wish. Justice could also seek direction from the Court in the form of a practice direction or annotated standard warrant templates,[341] or the bench and bar system recommended by the Segal report.[342]

g. Doubts Arising on Warrant Execution

225. (~~S~~) Once a judge issues a warrant, CSIS may execute the warrant. That execution must comply with the scope and terms of the warrant. After the warrant's issuance, CSIS and Justice conduct a debrief with the affiant, lawyer, the relevant headquarters desk and the responsible officials at the regions. This process includes a "reading of the warrant", designed as NSIRA understands it, to help inform execution. NSIRA was told that this debrief is sometimes regarded as vague and unhelpful, and that those charged with overseeing warrant execution had no resources to translate "warrant language" into techniques and powers they could use.

226. (~~S~~) The warrant coordinators in the regions lack formal training, and learn their task on the job – existing training is too broad and abstract, unconnected to the practical scenarios arising in the execution of warrants[343]. In consequence, expectations accrue as myths rather than clearly understood legal standards. NSIRA was told there were perceived disparities between what seemed to be on the face of the warrant and what lawyers described as the judge's intent. This sort of ambiguity reportedly gives rise to "invisible rules".[344] The regions are extremely uncomfortable with implied permissions, preferring tangible authorizations in warrants.[345]

[discussion of the detrimental effects on and risks to operations] [346]

227. **(U) Finding no. 21: NSIRA finds that the CSIS regional warrants coordinators have not received sufficient training enabling them to translate the contents of the warrants into advice on proper warrant execution.**

Recommendation no. 17: NSIRA recommends that CSIS regional warrants coordinator positions receive adequate training, and that CSIS professionalize the position and enable warrant coordinators to more effectively translate the content of warrants into advice on warrant execution.

339 Interview(s).
340 Interview(s).
341 Interview(s).
342 Interview(s).
343 NSIRA has been recently informed by CSIS that the lack of formal training also extends to warrant coordinators at headquarters (HQ). CSIS Factual Accuracy Check, December 22, 2021.
344 Interview(s).
345 Interview(s).
346 Interview(s).

C. Investment in People: Training

228. (S) As the discussion in this report demonstrates, training and institutional knowledge are recurring themes in this review. Most interviewees noted that they had not received specialized training prior to assuming their specific role in the warrant process, instead learning through word of mouth from others doing the same function. Some interviewees clearly felt unprepared for their role, and regretted the absence of systematic training. Several others tied the lack of training and the paucity of modernized processes and policies to compliance failures.[347] CSIS is to a certain extent alive to the shortcomings in its training programs and has itself noted that:

> *"CSIS is currently not a learning organization and does not have a learning culture. There are insufficient training opportunities to build and sustain a modern professional intelligence service that operates in a continuously evolving and complex environment, it is evident that the exponential needs across operational and corporate requirements has not kept pace with the current L&D staffing and funding allocation".*[348]

229. (U) The inadequacies of training featured in a recent internal review of the warrant process. NSIRA embraces its recommendations on the need for reform in this area.[349] NSIRA emphasizes especially, however, the need for education through scenario-based learning, and not simply training through the passive consumption of learning materials.

230. (S) CSIS's Learning and Development (L&D) branch has considerably revamped both the intensive program taken when employees join CSIS as Intelligence Officers (IOs), and the intensive course IOs take after several years at headquarters, before deployment to the regions. For instance, the IO Entry Training (IOET) which is largely content and theory heavy, is being overhauled to include scenario-based learning. L&D has embraced learner-centered approaches, with high instructor to trainee ratios. In its most recent iteration, the [training program name] now trains IOs in scenarios relevant to the duty of candour, including [training program content] capturing details related to legal credibility and conditioning passing grades on responsiveness to these matters.

231. (U) Trainers – IOs themselves participate in train-the-trainers programs. These trainers may themselves cycle to operational roles, where they are well-positioned to transmit expertise and mentor others. Meanwhile, NSLAG will work with CSIS's policy centres and provide feedback on learning modules raising legal issues. The [Name] will raise issues that may involve legal dilemmas. However, [Name] training does not address legal issues *per se* – rather the purpose is to train IOs in recognizing legal doubt, necessitating consultation with NSLAG. IOs are not trained, in other words, on answers to legal questions, so much as trained to recognize the existence of legal issues. Precise legal answers, it is feared, change with time, and a decision has been made to train a reflex to seek legal answers from NSLAG.[350] NSIRA notes, however, that the IOET and the [Name] come relatively early in an IO's career and that CSIS has no ongoing, formal professional development requirements[351]. NSIRA further notes that warrants-related training including duty of candour is of sufficient importance to necessitate annual mandatory warrant training for all operational personnel. This would allow operational personnel to remain apprised of changes in the warrants process as well as changes in the

---

347 Interview(s).
348 CSIS Business Case, Learning and Development: Building Foundations and Empowering Employees. Mar 31, 2021.
349 M.Rosenberg. Independent Review: Duty of Candour at CSIS, 2020 03 03.
350 L&D Briefing July 25, 2021
351 NSIRA notes that as of September 2021, CSIS began the delivery of a training workshop to be completed on an annual basis by all operational employees. Ref: CSIS Factual Accuracy Check, December 22, 2021.

operational environment including technological advancements which may influence their assessment of when a warrant is required.

232. (S) Aside from IO training early in an IO's career, specialized training in CSIS's various specialized trades is uneven. Most of the interviewees indicated they had received no formal training beyond that at the beginning of their careers, with a few exceptions (such as [Branch Name]).[352] Where there is in-house training, NSIRA's view is that it is often relatively informal and lacks some of the experiential features that the modern [Name] has developed. L&D is not responsible for training in specialized sub-trades or units of CSIS, although they may be consulted on design such that unit wish to establish a training system. This creates a gap in training for individuals who are not within the IO career stream.

233. (S) Following 2020 FC 616, CSIS implemented organization-wide mandatory training for all operational employees on the duty of candour. The thirty-minute training was contained in an online module that employees complete.[353] The module contains 22 slides discussing the duty of candour, including prior breaches and the role of every individual in ensuring that duty of candour is met. The module contains only two theory-based questions, no scenario-based training and may be completed in half the time by employees.[354] This type of training reflects concerns voiced during the review that CSIS cannot build a compliance culture by PowerPoint training,[355] and complaints that training included too much *pro forma* box checking.[356]

234. (U) In sum, the training culture at CSIS has been largely a "once and done" approach to formal skills acquisition. Moreover, NSIRA was led to believe that prior generations of the entry level and pre-regional deployment training courses were less robust than the present generation, and depended on more passive forms of education (such as PowerPoints). Bringing modernized training to more advanced IOs and standardized training of any sort to non-IOs appears to remain a challenge. L&D is not adequately resourced at present to expand a formal CSIS training footprint, despite considerable demand for specialized training.[357] Noteworthy, L&D has recently received CSIS management approval for their business plain to establish three regional training hubs to incorporate modern training at the regional level and enhance the skill set of IOs whose training may predate the existing training curriculum.[358]

235. (U) While both IOs and non-IOs noted the lack of training as a major issue, it was more pronounced with non-IOs. NSIRA heard from non-IOs including managers, analysts and technical experts that they did not receive the benefit of any form of formal training upon joining the organization.[359] Many had to ask for specific mentorship, while others have found that they are regarded as the most senior subject matter experts, leaving them with no mentorship options.[360]

236. (U) NSIRA observes that a commitment to training is only as real as the importance and resources devoted to it. Accordingly, training will succeed only to the extent that employee time is freed up to allow the acquisition of new skills and knowledge. In this respect, some

---

352 Interview(s).
353 L&D Briefing (25-07-21); Interview(s).; Project [redacted] DUTY OF CANDOUR 101[redacted] training course.
354 Project [redacted] DUTY OF CANDOUR 101[redacted] training course. CSIS has recently added duty of candour scenarios to it annual operational training workshop (see ft 351 above), Ref: CSIS Factual Accuracy Check, December 22, 2021.
355 Interview(s).
356 Interview(s). Project [redacted] Duty of Candour 101, [redacted] training course.
357 L&D Briefing (25-07-21)
358 CSIS Business Case, Learning and Development: Building Foundations and Empowering Employees. Mar 31, 2021. Business case approved on November 25, 2021. Ref: CSIS Factual Accuracy Check, December 22, 2021.
359 Interview(s).
360 Interview(s).

interviewees expressed doubt that units already confronting personnel shortages will succeed in building human capital.[361]

237. **Finding no. 22: NSIRA finds that CSIS lacks long-term training programs for Intelligence Officers.**

238. **Finding no. 23: NSIRA finds that CSIS has failed to provide systematic training programs for "non-Intelligence Officers".**

239. **Finding no. 24: NSIRA finds that the CSIS's Learning and Development Branch has not been sufficiently resourced to develop and administer comprehensive training programs, especially in specialized areas not covered by the training offered for Intelligence Officers early in their career.**

In view of these findings, NSIRA recommends that:

Recommendation no. 18: CSIS adequately resource and regularly deliver evergreen scenario-based training programs for all CSIS employees, including;

- **annual, comprehensive, warrant training for all operational employees;**
- **specialized onboarding training for all employees not part of the Intelligence Officer program; and**
- **continued long-term training for all specialized personnel.**

V. CONSEQUENCES OF SYSTEMIC PROBLEMS

240. (U) This report ends with an examination of, and associated observations on, cross-cutting governance and cultural issues that stem, at least in part, from challenges characterizing the provision of legal advice and the warrant process. NSIRA divides these broad, cross-cutting phenomena into two categories: morale and attitudes; and, performing the mission.

A. Morale and Cultural Resistance to Change

241. (U) NSIRA heard and read much about very low morale at CSIS -- a central concern not only to individuals whom NSIRA interviewed but also in employees' resignation and retirement exit interviews.[362] There are likely many reasons for this morale problem. The systemic and governance issues in the warrant process are part of them. Morale is injured by a warrant acquisition system that seems to impede performance of the mandate while at the same time being the source of regular reputational crises stemming from duty of candour failures.

242. (U) At the same time, employees see themselves as participating in a rigorous process. Indeed, so rigorous is this process that employees are frustrated that too few warrants are

[361] Interview(s).

[362] Employee Exit Interviews # 5, 7, 9, 11-14,18, 19, 23, 24, 35, 39, 48, 50, 57, 63-70, 74.
The morale issues noted in this section are also evidenced in the Public Service Employee Survey Results for CSIS for 2020.

being sought. They feel caught in a no-win environment compounded by the bureaucratic burden associated with having a warrant application reach the Court.

243. (U) NSIRA notes that those disillusioned by seemingly unending compliance issues reportedly fall into three categories, reflecting sometimes quite different perspectives: those viewing compliance measures as an inconvenience; those who do not understand the purpose of compliance measures; and, those who viewed them as a manifestation of diffused or insufficient governance responsibility.[363]

244. (U) First, some interviewees stated that, while duty of candour failures at the Federal Court have resulted in further disclosure obligations and demanded additional undertakings,[364] these failures are perceived as a risk to be managed rather than a problem to be solved.[365] For this group, the implication is that the rule of law is not a grounding consideration.[366] Indeed, some interviewees did doubt the existence of a compliance culture, or that compliance with duty of candour standards was embraced seriously as part of confidential source management.[367]

245. (U) Others had very different views, and regarded compliance failures as tied to the lack of training and the paucity of modernized processes and policies.[368] CSIS has historically under-resourced policy, compliance and training.[369] Even where policies are changed, NSIRA was told that simply announcing new protocols cannot effect change – and indeed, they may go unread.[370] Some interviewees reported, for example, that Project [Name] communications are ignored.[371] CSIS is developing policy centres, but employees may have a foggy understanding of the role of these units, and may not be sufficiently attuned to issues to know when to seek expert input.[372]

246. (U) With regards to the third category, NSIRA heard concerns about flawed governance in warrant and compliance matters. Some interviewees expressed concern about governance vacuums. In the eyes of some, managers have done too little to redress employee uncertainty about rules, and indeed even managers at the executive level reportedly sometimes lack understanding of applicable rules.[373] NSIRA heard concerns that employees are reportedly not rewarded for compliance initiatives, and indeed some personnel implicated in poor compliance conduct have been promoted.[374] CSIS was described by some as possessing a culture in which bad news does not travel upwards, and one in which managers resist lessons-learned analysis and reporting, and prefer positive spins on errors.[375]

247. (U) For other interviewees, CSIS allegedly has a zero-fail approach to some compliance issues, producing a brittle, risk averse working environment. For instance, within CSIS there is reportedly no attitude that in litigation, one wins some and loses some.[376] A troubled warrant application is widely regarded as disastrous, and career impairing. Indeed, interviewees

---

363 Interview(s).
364 Interview(s).
365 Interview(s).
366 Interview(s).
367 Interview(s).
368 Interview(s).
369 Interview(s).
370 Interview(s).
371 Interview(s).
372 Interview(s).
373 Interview(s).
374 Interview(s).
375 Interview(s).
376 Interview(s).

described an internal fear of making mistakes, and a punitive, "call out" culture when mistakes are made.[377] The aim is "not to fail" in order to be promoted, leading to a cautious culture in which some people prefer not to act or ask questions.[378] This culture likely undergirds the multiplicity of warrant steps, and the diffusion of responsibility. It may also be a partial explanation for why some legal doubts are not brought before the court for resolution through the warrant process.[379]

248. (U) In crafting its recommendations, NSIRA aligned the core warrant responsibilities to the legislative accountability framework while ensuring that those controlling the process can set a careful watch over one of the drivers of morale within their organization.

B. Performing the mission

249. (U) In this report, NSIRA has identified several governance and cultural problems. The lack of alignment in the way Justice provides legal services with the needs of CSIS, the delay inherent to the quest for legal advice, and the disconnect between the content of legal advice and the operational imperatives of CSIS may not completely explain the current climate. However, this situation can only have compounded other possible causes, if any, beyond the parameters of this review. The problems have resulted in a culture of distrust towards Justice counsel and a systemic reaction whereby CSIS sometimes avoids seeking legal advice.

250. (U) While NSIRA does not question the need for Justice to speak with "one voice", the governance structure put in place to safeguard consistency cannot override another fundamental goal, which is to allow its client to comply with and to respect the rule of law.

251. (U) To become "client-centric" as promised in Justice's VISION Project, Justice must go from being perceived as a roadblock, to a frank and forthright advisor fully attuned to operational objectives. To achieve that goal, several interconnected recommendations of this report need to be implemented. They reach into Justice's governance and culture. On the governance aspect, they relate to training, to prompt and clear advice-giving, and to early and extended availability of counsel. On the culture aspect, they relate to the culture of support that goes beyond the mere provision of legal opinions constituting traffic signals – they call for counsel working as advisors opining in an iterative manner on how an intelligence operation might proceed in a manner that respects the rule of law. Providing road map-style advice does not mean Justice abandons its fearless defence of the rule of law, or its independence. It does mean that it situates this advice in a manner that best serves the shared goal of operations compliant with the rule of law. Changing the culture of distrust and avoidance can take time, but early, continued and consistent engagement in operations should contribute to rebuilding the relationship.

252. (U) The current governance of advice-giving is unnecessarily detrimental to operations. If the course is not corrected, both organizations put at risk the fulfillment of their mandates.

253. (U) For CSIS, the risks to its fulfillment of its mandate arise on multiple fronts. NSIRA endorsed above the view that warrants are the "lifeblood" of CSIS. CSIS members may, however, vary in the degree to which they appreciate the significance of warrants. Many interviewees adhered to what may be called a national security culture, in which success is about leveraging CSIS's mandate to contribute to Canada's national security. The objective is to provide useable, lawfully-collected information of value to the government of Canada.[380] In

---

377 Interview(s).
378 Interview(s).
379 Interview(s).
380 Interview(s).

this view, the entire CSIS apparatus needs to understand the objectives behind the collecting of information, and see itself as engaged in a collective enterprise, rather than discrete, atomized endeavours. Disillusionment, NSIRA concluded, often reflected recognition of how warrants (and law) are increasingly important in intelligence operations, but at the same time hard to obtain. With the increasing dominance of electronic communications, what was once standard pre- or non-warranted tradecraft is now increasingly crossing the line into activities requiring warrants.[381] Warrants, in other words, reach far into CSIS's traditional tradecraft.

254. (U) It was, however, the considered opinion of a number of our interviewees that too many CSIS investigations are now stranded by the warrant process. That process was sometimes compared to winning a lottery,[382] not because of lack of success at the Federal Court but because of the resource intensity of getting the application to the Court.[383]

255. (S) NSIRA was also advised of investigators [discussion of how collection activities are affected] doing their best to advance investigations [discussion of effects on collection activity]. Leaving to individual interpretation which [collection activity] may be used could result in boundaries being pushed, compounding grey zone legal issues and reputational risk if these practices then culminate in review or court proceedings.[384] Further, while warranted collection might clarify whether CSIS's reasonable belief that the individual is engaged in threat activities is well-founded, other techniques may leave the target in limbo. [discussion of how collection activities are affected] . At the same time, it risks focusing the state's attention on people for greater periods of time because [discussion of how collection activities are affected][385]

256. (U) There was widespread support for the view that the warrant process should not be the bottleneck on warranted activities – that any bottlenecks should be driven by operational imperatives.[386] NSIRA was told the metric of success for a reformed warrant process amounts to: more warrants, more closely tailored to the threat, with shorter and more detailed threat assessments that simultaneously meet the court's expectations.[387]

257. (U) As the calculations in the preceding sections show, the question of how many warrants CSIS should transact annually was not easily answered. The near-consensus was, more than the number that have been sought in the recent past. The expectation is that operational imperatives in an era of complex threats and burgeoning electronic communication will require more warranted activities. The number of novel issues can only increase, compounding the need for legal advice, which highlights the need for cooperation with Justice.

258. (U) Given the challenges identified in this report, NSIRA could detect no clear path to achieving such an objective under the *status quo*. In these circumstances, the warrant process risks remaining the worst of all worlds: a system that makes it too hard for CSIS to perform the mandate given to it, while at the same time doing too little to safeguard against legal error.

259. (U) This report has identified many governance issues at both Justice and CSIS. The deficiencies in information management; the lack of training; the multiple steps in the warrant process; the absence of an efficient challenge function; the lack of understanding of the decision-making process; and the absence of clear accountability lines all go to the heart of the

381 Interview(s).
382 Interview(s).
383 Interview(s).
384 Interview(s).
385 Interview(s).
386 Interview(s).
387 Interview(s).

very questions that characterize the notion of governance: How are decisions made? Who makes them? Who is accountable for them?

260. (U) Reforms should allow for clear answers to these questions. Among other things, NSIRA has recommended that the CSIS Director assume more immediate responsibility for the Affiant Unit and that the Minister and Public Safety host a more immediate role in challenging warrants. These structural reforms, however, will only produce positive changes if accompanied by the implementation of the other recommendations, especially those sustaining the Affiant Unit.

261. (U) In sum, this review was sparked by a compliance failure in a duty of candour matter. It concludes that repeated failures in this area are both caused by, and cause, deep-seated governance and cultural patterns. This vicious cycle has compounded the challenges of reform in the warrant acquisition process. NSIRA agrees with the 2020 Rosenberg Independent Review that "a precondition to successfully implement the recommendations is to address the cultural issues around warrants".[388]

262. (U) The challenges communicated by many interviewees will not disappear unless widespread governance reforms facilitate an improved warrant process. Cherry-picked changes or paper reforms that mask governance and cultural issues, without addressing them, will suffer the ignominious fate of prior rounds of changes: they will not fix systemic issues. This will require a major effort. In this review, NSIRA has proposed a series of reforms. No single recommendation made here will alone resolve the source of systemic issues in the warrant process. CSIS and Justice shall need to pursue recommendations as a package.

263. **(U) Finding no. 25: NSIRA finds that CSIS and Justice are at risk of not being able to fulfill their respective mandates. No one reform is likely to succeed unless each is pursued as part of a coherent package. No package will succeed unless backed by prioritization at senior levels, and the stable provision of resources, including people with the means and institutional knowledge to see reforms through. And no reform initiative will succeed unless accompanied by clear performance indicators, measured and analyzed regularly to track progress.**

In view of NSIRA's findings above, and of prior unsuccessful reforms, NSIRA recommends that:

(U) Recommendation no. 19: The recommendations within this review be treated as a coherent package and that progress and outcomes in implementing these recommendations be tracked, allowing management, the Ministers of Public Safety and of Justice, and NSIRA, to assess the efficacy of reforms and course correct if necessary.

264. (U) NSIRA intends to launch a follow-up review, within two years, which will measure progress at CSIS, Justice and Public Safety in resolving the systemic issues with the warrants process addressed by this review. Moreover, in other regular reviews implicating warrants, NSIRA will document recurrences of systemic problems. In the meantime, since this review originated with

[388] M. Rosenberg; Independent Review: Duty of Candour at CSIS. 2020 03 03 at slide 3.

a decision of the Federal Court, it is vital that the Minister and CSIS share it in its full form with the designated judges of that court.

In recognition of the fact that this report followed a recommendation of the Federal Court, NSIRA in turn recommends that:

(U) Recommendation no. 20: The full, classified version of this report be shared with the designated judges of the Federal Court.

ANNEX A: Historical Initiatives:

	Year	Event	Summary	Response
1.	1987	DoC[389] Breach	Atwal:[390] ▪ Harjit Singh Atwal was the subject of a Federal Court (FC) issued warrant in July 1985. ▪ In September 1987, the Court was advised that extensive errors had been discovered by CSIS in the warrants application, such that there would be insufficient information for the warrant to issue. ▪ This resulted in the FC setting aside the warrant in October 1987.	▪ The Director of CSIS resigned. ▪ A mass review of information used in support of issued warrants was conducted. ▪ A new internal requirement for an Affidavit Content Certificate signed by four individuals certifying the facts alleged and the need for the powers sought was imposed.
2.	1992	Report	The Addy Study:[391] ▪ In 1992 on request of CSIS, George Addy (retired FC Judge) conducted a review of the CSIS warrant acquisition process. ▪ The report was highly critical of the warrant acquisition process especially the number of steps and people involved in the process ([redacted] steps with a minimum of [redacted] people). ▪ The report provided 20 recommendations including:	▪ CSIS's 1993-1994 annual classified report to the Minister noted that in response to the Addy study "new and slightly amended procedures came into effect on November 1, 1993."[392] The new approach was designed to streamline the process and add flexibility in scheduling in order to align average processing time to that suggested by the Addy study.

[389] Duty of Candour (DoC).
[390] *Atwal v. Canada,* [1987] F.C.J. No.901 (T.D.).
[391] *Study of, Report on, and Recommendations Relating to Process for Acquisition of Warrants by CSIS*, George Addy, 1992.
[392] CSIS annual report 1993-1994, May 25, 1994.

			- Questioning the utility of Independent Counsel (IC). - Only those whose normal responsibilities contribute something to the warrants process, should be included in that process. -Those involved in the process should have the time to conduct their task without regard to seniority or to normal operational hierarchy. -Improved communication between the region and Headquarters (HQ) throughout the warrant process. -The attitude that blame must result as a matter of course from any Court refusal or variation of an application, should be abandoned. -Where there is legal ambiguity, the matter should be submitted to the Court. -[timeline] should be the absolute maximum for the time required to obtain any warrant.	
3.	2004	DoC Incident	[redacted]: ▪ In 2004, CSIS informed the Court of inaccurate information contained in a warrant application.[393] ▪ Counsel went before the Court and reported on internal efforts taken to prevent the recurrence of such errors. ▪ The Court issued a Direction requesting that these internal efforts be provided to the Court in written format.	▪ On September 12, 2004, Counsel for CSIS wrote to the FC[394] to assure the Court that enhanced checks on warrant applications had been implemented including: - Regional review of draft warrant (including the assigned investigator). - Counsel ensures final comprehensive personal review of documentation. - Counsel meets with the analyst and affiant to review the application prior to filing.

[393] [redacted]

[394] Letter from John O'Halloran to the Federal Court September 12, 2004. [redacted]

4.	2004	DoC Incident	[redacted][395] ▪ In June 2004, the FC issued a warrant, [redacted]. ▪ The 2005-2006 Office of the Inspector General (OIG) review of the CSIS investigation related to the issued warrant, noted that significant information in support of the application should have been included in the affidavit.	▪ The Director of CSIS wrote to the FC informing the Court of the [redacted] additional pieces of information that were in CSIS's possession yet not included in the affidavit.[396]
5.	2005	DoC Breach	[redacted][397] ▪ In June 2005, the FC dismissed an application for a warrant. This was due to the failure to provide full, fair and accurate information to the Court. ▪ Information included in one of the paragraphs of the affidavit was misleading and failed to disclose material facts. ▪ A subsequent CSIS review of the affidavit identified [redacted] sources of information that should have been included in the affidavit.	▪ The Director of CSIS wrote to the FC apologizing for the failure to provide "full, fair and accurate disclosure".[398] ▪ The letter sent to the FC outlined a number of steps taken by CSIS to address the candour shortcomings, including: - The imposition of an immediate moratorium on the filing of all warrant applications to allow for internal review of all affidavits to ensure that the DoC was met. - The Director briefed the Warrant Review Committee (WRC) on the importance of full, fair and accurate disclosure. - Senior Counsel was asked to review the warrant process (see below at 6).

[395] Office of the Inspector General of CSIS, 2005-2006, Review of CSIS Investigation of [redacted] 11/09/2006.
[396] *Ibid*.
[397] *Supra* 1.
[398] Letter re: [redacted] and the integrity of the warrant application process from CSIS Director to Federal Court Chief Justice, July 25, 2005.

				- Senior Counsel was asked to arrange awareness sessions. ▪ The moratorium imposed by the Director of CSIS was short lived and replaced in July, 2005, with a moratorium letter. This required that a letter be filed with the notice of application indicating that the Director was personally satisfied that the documents submitted to the Court met the obligation that CSIS provide full, fair and accurate disclosure of all material facts.[399] ▪ The moratorium letter requirement ended in June, 2006.[400]
6.	2006	Report	[Summary of Internal Review]	▪ The report was widely circulated throughout CSIS and the Department of Justice (DoJ). ▪ CSIS did not implement any substantial changes in response to the report.

[399] Letter re: Moratorium on CSIS Warrant Applications from General Counsel to the Federal Court, October 13, 2006.
[400] Email from [redacted] to [redacted] Director's moratorium on Warrant Applications 2005/2006, 2018-10-17.
[401] [redacted]

			[Summary of Internal Review]	

			[Summary of Internal Review] [redacted]	
7.	2008	DoC Incident	Multiple Warrant Errors, OIG 2007-2008:[402] ▪ In 2008, the OIG examined [redacted] CSIS affidavits and identified [redacted] errors in the applications. While some of the errors were minor typographical errors, others were more substantive, such as the attribution of comments made by the investigator to the target.	▪ CSIS wrote to the FC advising it of the errors identified by the OIG and the measures they intended to implement internally to improve facting for the warrants process. ▪ The proposed measures included: - Enhanced training for affiants and analysts to improve verification techniques and foster accountability for completeness of information.

[402] Office of the Inspector General of CSIS, Warrants Review, July 1, 2006 to June 30, 2007 (October 27, 2008).

				- Assignment of a senior investigator to challenge the accuracy of the application prior to its filing. - Conducting spot audits of representative affidavits.
8.	2009	DoC Breach	*Harkat (RE)* 2009 FC 1050: ▪ On May 26, 2009, CSIS informed the FC that it had failed to disclose that one of the key human sources used in the Harkat Security Certificate case had failed a polygraph test. The information was brought to the Court's attention months after the Court had asked a CSIS witness questions pertaining to the reliability of the source.[403] ▪ The Court concluded that the witness did not intend to mislead the Court, and that the issue was in part "an institutional failure of CSIS." ▪ In its decision, the Court noted, "the failure of CSIS, and of its witnesses, to act in accordance with the obligation of utmost good faith…has undermined the credibility of this Court's process."[404]	▪ On June 4, 2009, Senior Counsel for CSIS wrote to the FC to address the non-disclosure.[405] The letter acknowledged that the issues related to the source matrix (credibility) noted by the FC may give rise to questions regarding the integrity of the source materials filed in security certificates before the Court. ▪ In the letter CSIS committed to: - Reviewing and internally challenging all the source matrices and supporting human source files. - Expanding the role of the IC (to include challenging the source matrices used in warrant applications). - Reviewing internal practices concerning the presentation of evidence in Court to prevent similar omissions in the future. ▪ Following receipt of the letter, the FC issued a direction requiring that all applications are to be accompanied by a letter from Senior Counsel for CSIS assuring the Court that the Director is satisfied that the application meets

[403] SIRC Study 2011-02.
[404] *Harkat (RE)* 2009 FC 1050 at para 59.
[405] Letter from CSIS General Counsel to the Honourable Allan Lutfy, June 4, 2009.

				CSIS's obligation to act in utmost good faith and make full, fair and candid disclosure of facts including those that may be adverse to its interest. ▪ The subsequent CSIS internal review of the procedures related to the preparation of human source précis concluded that: "the lack of centralized control and coordination over source précis led to inconsistencies in both format and content, and could impact on its capacity to meet requirements for full, fair and frank disclosure as they apply in relation to assessments of the reliability and credibility of the Service's human sources and their information."[406]
9.	2009	DoC Breach	*Almrei (RE)* 2009 FC 1263: ▪ In 2009, the FC found that CSIS failed to provide exculpatory information related to the Human Sources relied upon in the Almrei Security Certificate case. ▪ The FC judge noted that information contained in the Security Intelligence Report included "information that could only be construed as unfavourable to Almrei without any serious attempt to include information to the contrary."[407]	▪ CSIS developed policy to govern the preparation of the human source précis. ▪ CSIS developed a training program focused on promoting "rigour" in all activities.

[406] Letter from CSIS General Counsel to the Honourable Allan Lutfy, May 20, 2010.
[407] *Almrei (Re)* 2009 FC 1263, paras. 503, 500.

			▪ In its decision, the Court found that CSIS and the Ministers had breached their duty of candour to the Court.	
10.	2013	DoC Breach	2013 FC 1275: ▪ On May 4, 2009, the Court issued reasons for a warrant to intercept foreign telecommunications from within Canada. This warrant was initially issued in January, 2009, and further renewed on April 6, 2009. ▪ The warrant was authorized on the basis that the interception of foreign communications would be conducted from within Canada. Several other warrants were issued on this basis. ▪ CSIS failed to bring to the Court's attention that requests would be made to foreign partner agencies to intercept the communications of the individuals subject to the warrant. ▪ The Court noted that the failure to disclose information material to the application "was the result of a deliberate decision to keep the Court in the dark about the scope and extent of the foreign collection efforts that would flow from the Court's issuance of a warrant."[408] ▪ The Court found this to be a breach of the duty of candour owed by CSIS and its legal advisors to the Court.	

[408] 2013 FC 1275, at para. 117.

11.	2014	DoC Breach	[redacted] Prosecution: ▪ In 2013, the Ontario Superior Court of Justice noted a discrepancy in a CSIS affidavit for warrants. ▪ In February 2014, the FC requested that CSIS provide information on the steps taken to: bolster the accuracy of information to obtain a warrant; improve the overall process for warrant acquisition; and record the exchanges of information with law enforcement officers.	▪ In April 2014, CSIS provided a report to the Court outlining the safeguards in place within the warrants process, to challenge and assess the reliability of information placed before the Court. ▪ In July 2014, the Director of CSIS issued a reminder to all employees regarding the duty of candour obligations to the Security and Intelligence Review Committee (SIRC) and the Court, including information that may be adverse to CSIS's interests.
12.	2014	DoC Breach	SIRC Decision, Complaint reports/SIRC Annual Report 2013-2014: ▪ In one complaints investigation report, "SIRC found that it had been seriously missed by CSIS and that CSIS had violated its duty of candour during *ex parte* proceedings by not proactively disclosing in its evidence its rejection of the reliability of a source of information."[409] SIRC noted that CSIS's lack of candour was most disturbing.[410] ▪ In another complaints investigation report, SIRC was critical of CSIS failing to proactively highlight a highly relevant document. SIRC reminded CSIS that its	▪ Please see July 2014 internal reminder to all employees noted above.

[409] 2013-2014 SIRC Annual Report, p. 3.
[410] *Ibid.* at p. 29.

			disclosure obligations went beyond producing a large quantity of documents for SIRC's review and included the duty to proactively present the most relevant pieces of evidence before any presiding Member.[411] ▪ In responses to the noted candour incidents, SIRC recommended "that a policy directive be issued to all CSIS personnel about the importance of the duty of proactive candour in proceedings before SIRC."[412]	
13.	2016	DoC Incident	[redacted] ▪ On January 7, 2016, the FC issued a lengthy order regarding misrepresentations to the Court of information within [redacted] warrant applications. ▪ The order required that additional human source and domestic/foreign agency information be filed with the Court. ▪ Additionally the Court ordered that CSIS provide a written rationale to address both the omission of information and the misleading application.	
14.	2016	DoC Breach	2016 FC 1105 (*Associated Data Decision*): ▪ In 2016, in response to the 2014-2015 SIRC Annual Report[413], the FC convened an *en banc* hearing of designated judges. In October, 2016, the FC issued an *en banc* decision.	▪ In response to the Court's ruling, the Minister of Public Safety invoked a formal request to

[411] *Supra* 20.
[412] *Supra* 20 at p. 30.
[413] 2014-2015 SIRC Annual Report. In the report, SIRC recommended that CSIS advise the Court of the particulars of the Service's retention and use of metadata collected under warrant. CSIS did not agree with the recommendation to inform the Federal Court. CSIS's position was that section 21 of the *CSIS Act* does not confer any general supervisory authority to the FC judges and that SIRC's recommendation was both inappropriate and unwarranted. CSIS stated that it "maintains that its position on the issue in question was communicated clearly and transparently to the Federal Court".

			▪ The Court found that CSIS had unlawfully retained non-threat and third party information that was linked to lawfully (warranted) collected communications. ▪ The Court noted that this associated data was non-threat related and therefore did meet the strictly necessary threshold for retention as per section 12 of the *CSIS Act*. ▪ The Court was not aware of the existence of this bulk data analytics program housed within a specialized branch called Operational Data Analysis Center (ODAC) or that associated data was unlawfully used and retained for over ten years through this branch. ▪ The Court found that CSIS had, again, breached its duty of candour. ▪ In a stern rebuke the Court, referencing the current and previous breaches of duty of candour noted "I wonder what it will take to ensure that such findings are taken seriously. Must a contempt of Court proceeding with all its related consequences, be necessary in the future?"[414]	SIRC under section 54 of the *CSIS Act* to review CSIS's response to the Federal Court. ▪ CSIS initiated a review of the business systems that underpin the collection and processing of information acquired pursuant to warrants. The review, named [redacted] provided a number of recommendations / courses of action. Based on the course of action selected by the executive, a number of smaller projects were launched, but many remain incomplete.
15.	2016	Report	Review of CSIS Warrant Practice, Murray D. Segal[415] (Segal Report)*:* ▪ This review was conducted at the DoJ's request, with the objective of seeking advice on best practices in *ex parte* matters by examining the CSIS warrant process. ▪ The review examines the duty of candour requirements	(2017): Advice on implementing the recommendations of Murray D. Segal's Review of CSIS Warrant Practice, John H. Sims:[416] ▪ In response to the Segal Report, the DoJ requested a subsequent report on implementing the Segal Report and managing

[414] 2016 FC 1105 *(Associated Data Decision)*, paras. 107-108.
[415] Review of CSIS Warrant Practice, Murray D. Segal, December 2016.
[416] *Advice on Implementing the Recommendations of Murray D. Segal's Review of CSIS Warrant Practice*, John H. Sims, March 2017.

			and provides pertinent observations regarding cross-jurisdictional best practices. ▪ The review provides twenty-one recommendations many of which echo observations and recommendations made in previous reviews. ▪ The recommendations include: - Affiants must be equipped with a profound understanding of the DoC and sufficient skill and experience to successfully implement it. - CSIS should ensure that the role of affiant is a senior and respected role within the Service, and that affiants occupy that role on a recurring basis. - The appointment of *amicus curiae* should be recommended where a warrant application raises novel and/or difficult legal issues. - The Court should be informed where CSIS has changed its legal position in respect of an issue before the Court. - The DoJ and CSIS should establish a formal joint policy on DoC in warrant applications. - A bench and bar committee should be established, with representations from "both" sides of the national security law bar. - The IC should be expanded to include scrutiny of legal and policy issues arising from a warrant application. - The IC should be empowered to recommend to Senior General Counsel that a request for the appointment of *amicus* be made to the Court. - A short list of Public Prosecution Service of Canada (PPSC) counsel with relevant expertise who are available on short notice to provide advice on difficult	warrant applications before the Federal Court *(Sims Report).*[417] ▪ The Sims Report was supportive of several of the Segal Report's recommendations including the need for increased training, the need for a joint policy/protocol on the DoC – to be renewed every 2-3 years, and the need for experienced affiants. ▪ The report does, however, differ on some issues, including the expanded role of IC. The Sim's report notes that the "NSG [National Security Group] counsel (IC) do not have the knowledge and experience in national security matters that could indeed be deployed productively in areas beyond their current mandate." Accordingly, the report recommended that the mandate of NSG be expanded incrementally to allow for growth in knowledge and experience. ▪ In 2017, *The Policy of the Department of Justice and CSIS on the Duty of Candour in ex parte Proceedings* (Joint Policy) was issued. The policy sets out the principles that should guide the discharge of the duty of candour by counsel acting for the Attorney General of Canada (AGC) and by CSIS witnesses and affiants.

[417] *Ibid.*

			warrant issues should be developed. - Secondment of CSIS counsel to other branches of Justice should be encouraged. ▪ Improved warrant training for CSIS employees and counsel.	
16.	2020	Report	Duty of Candour at CSIS, Independent Review, M. Rosenberg (Rosenberg Review):[418] ▪ From 2018-2020, the FC conducted a series of *en banc* hearings to address DoC issues pertaining to CSIS human source (HS) activities in three warrant applications. These hearings led to the breach of DoC decision (discussed below). ▪ While the three applications were before the Court, CSIS requested an independent review of the duty of candour at CSIS, specifically as it related to certain omissions of information pertaining to a HS in one of the warrant applications. ▪ The resulting report provides a number of recommendations, but notes that "a precondition to successfully implement the recommendations is to address cultural issues around warrants".[419] ▪ The report was critical of the culture surrounding warrants at CSIS. It noted that there has been inconsistent follow-through on DoC initiatives following the various breaches.	▪ In response to the Rosenberg Review, CSIS launched Project [redacted] This initiative seeks to implement the recommendations set out in the Rosenberg Review. ▪ This initiative is currently ongoing.

[418] *Independent Review: Duty of Candour at CSIS, Morris Rosenberg*, March 3, 2020.
[419] *Ibid.*, slide 3.

			▪ Much like former reviews, this review was critical of the affiant role, noting that it was perceived as a "side of the desk" task that takes away from intelligence work. ▪ Like the Duffy Report and the Addy Study before it, the report noted the lack of regional ownership over the warrant process. ▪ The Review makes four key recommendations, namely: employee engagement; improved training; clarification of roles and responsibilities (including implementation of the AU); and the implementation of audit, review, and compliance mechanisms. ▪ The Review makes several additional recommendations, including: - Changes to the HS process, including improved information verification and credibility/reliability issue awareness. - Regional engagement in the warrants process through feedback mechanisms from HQ and DoJ liaison access.	
17.	2020	DoC Breach	2020 FC 616: ▪ In 2018, during a CSIS warrant application before the FC, questions pertaining to HS operations and possible engagement in activities in contravention of the terrorist financing provisions of the *Criminal Code of Canada* arose. Although the warrant was issued, the FC expressed its dissatisfaction with the responses received and the candour to the Court. These issues re-emerged in the context of [redacted] further warrant applications, leading to an *en banc* hearing of 14 designated judges in 2019. Multiple evidentiary	▪ On June 23, 2020, in response to the Court's recommendation for an external review, the Ministers of Justice and of Public Safety and Emergency Preparedness referred the recommended review to NSIRA. ▪ Project [redacted] (see above).

			hearings followed over the next year until the issuance of the Court's decision in May 2020. ▪ In May 2020, the FC issued a decision dealing with the common issues before the Court. The lengthy decision includes a detailed background of how the Crown immunity issues transpired, the assessment of legal risk of operations, the warrant application process, the role of the DoJ and the institutional and systemic issues contributing to the breach. ▪ The Court noted "it is difficult to overstate how disturbing these circumstances are. Operational activity was undertaken in the face of legal advice to the effect that the activity was not authorized by the *CSIS Act*"."[420] ▪ The FC found that CSIS breached the duty of candour it owed the Court in failing to proactively identify that it had included in support of warrant applications information that was likely derived from illegal activities. - The Court recommended a review of the systemic, governance and cultural shortcomings and failures that resulted in CSIS engaging in operational activity that it conceded was illegal, and the resultant breach of candour.	
18.	2020	DoC Breach	2020 FC 119: ▪ On December 2020, the FC issued its decision in one of the warrant applications that was subject of the common issues decision in 2020 FC 616. ▪ In its decision the Court addressed both the potentially illegal activities of the HS discussed within the realm of	▪ Project [redacted] (see above).

[420] 2020 FC 616, at para 122.

			the 2020 FC 616 decision, as well as issues pertaining to the failure of CSIS to disclose information that may affect the Court's assessment of the human source's credibility and reliability. ▪ The source in question was also the subject of a high risk operation disclosed to the Minister prior to the warrant application yet this connection was never made at the Warrant Review Committee and never disclosed to the Court. ▪ The FC found that CSIS had breached the DoC it owed the Court by not disclosing that information it relied upon may have been derived from activities that potentially contravened the criminal code and by failing to disclose information that had the potential to adversely reflect in the reliability and credibility of the human source relied upon in its application. ▪ The FC noted that "due to the regrettable frequency with which the service has breached its duty of candour" CSIS and the AGC were ordered to keep the Court apprised of NSIRA's review in response to *2020 FC 616*. [421]	
19.	2021	DoC Breach	2021 FC 541: ▪ This was the final decision pertaining to one of the warrant applications before the Court in 2020 FC 616. The Court deferred to the decision on candour from 2020 FC 616. ▪ While the Court found that the warrants in question would have issued despite the candour breach relating	▪ Project [redacted] (see above).

[421] 2020 FC 119.

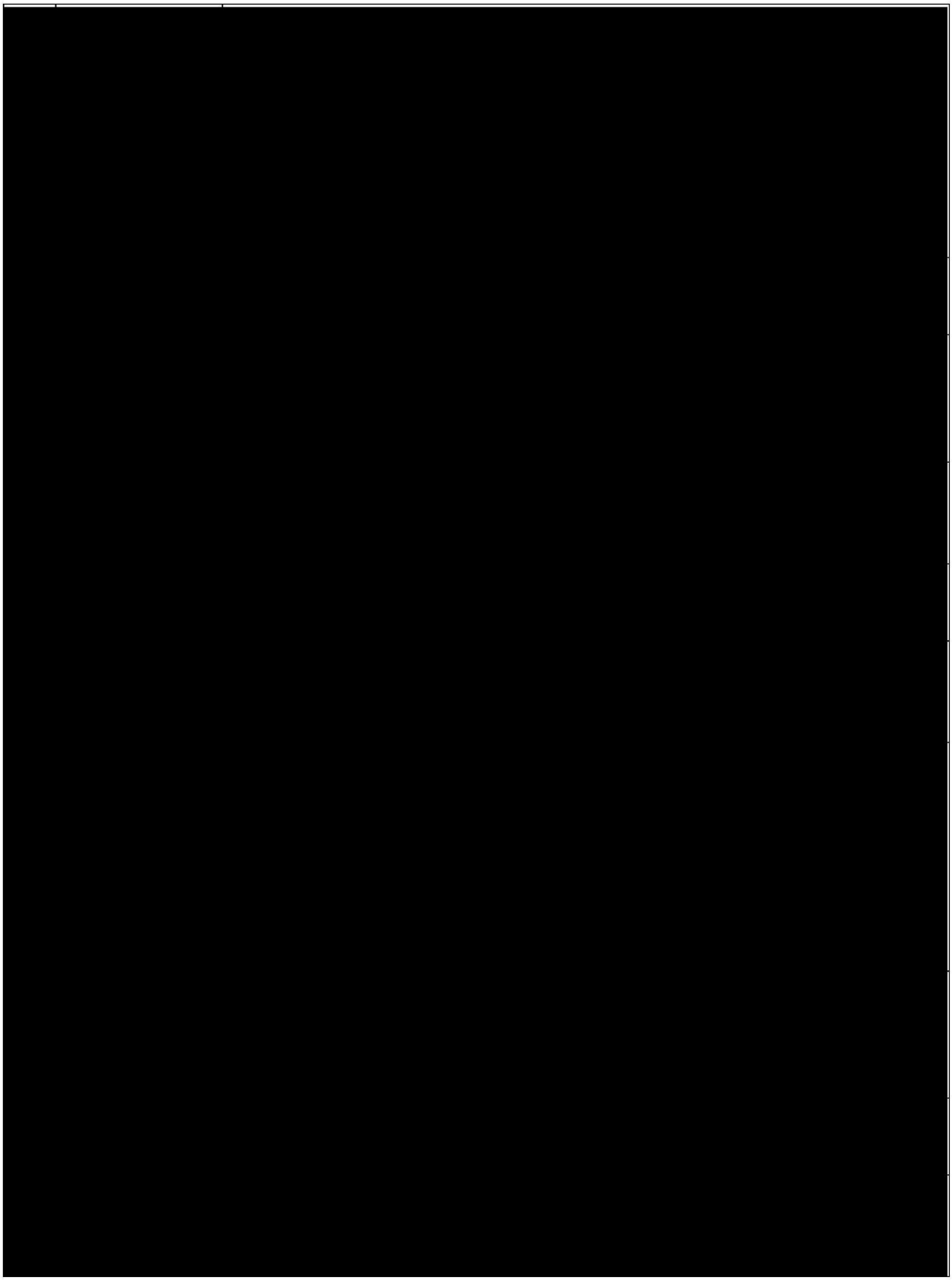
			to the omission/non-disclosure of information, the Court did assert "that in other circumstances the Court could fashion a remedy to address the non-disclosure of essential information."[422]	
20.	2021	DoC	2021 FCA 92: ▪ This decision was in response to the Appeal by the AGC of the 2020 FC 616 decision. ▪ The FCA found that that the Federal Court had erred in holding that the duty of candour required the Service to proactively seek waiver of solicitor-client privilege and disclose legal advice in a warrant application. ▪ The decision was specific to one of the three warrant applications initially before the FC and specifically pertains to "the treatment of the duty of candour issue as it related to the legality of the cover operation and the Service's reliance on information obtained through that operation".[423] ▪ This decision overturned the first paragraph of the 2020 FC 616 decision relating to the breach of duty of candour by CSIS in one of the warrants before the Court. The decision did not overturn the Court's initial recommendation that a comprehensive external review be initiated to fully identify systemic, governance and cultural shortcomings and failures that resulted in CSIS engaging in operational activity that it has conceded was illegal and the resultant breach of candour.	

[422] 2021 FC 541, at para 88.
[423] 2021 FCA 92 at para 88.

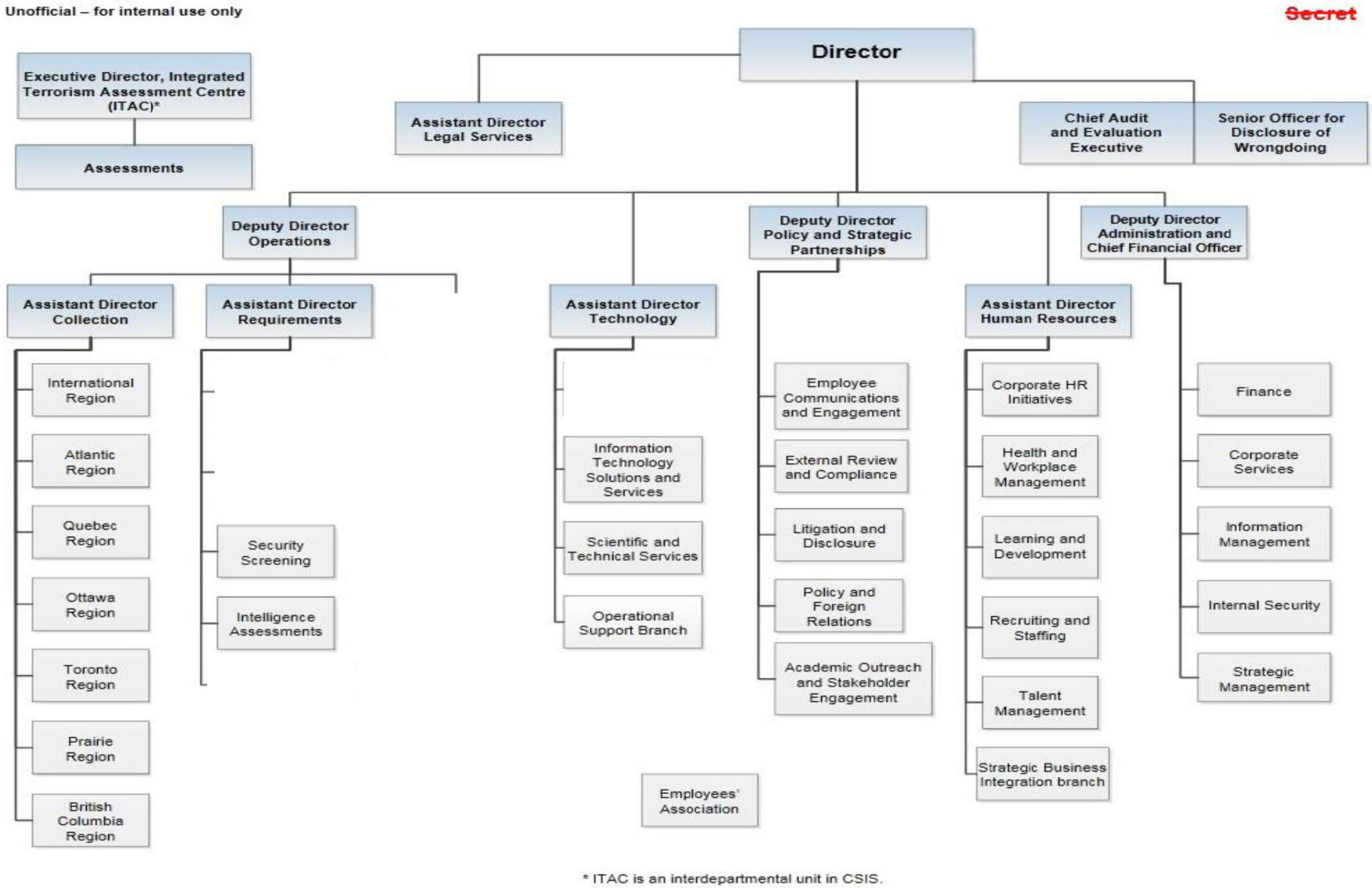
ANNEX B: Warrants acquisition schedule:

	Target Date	Deliverables
[redacted]		

[redacted]

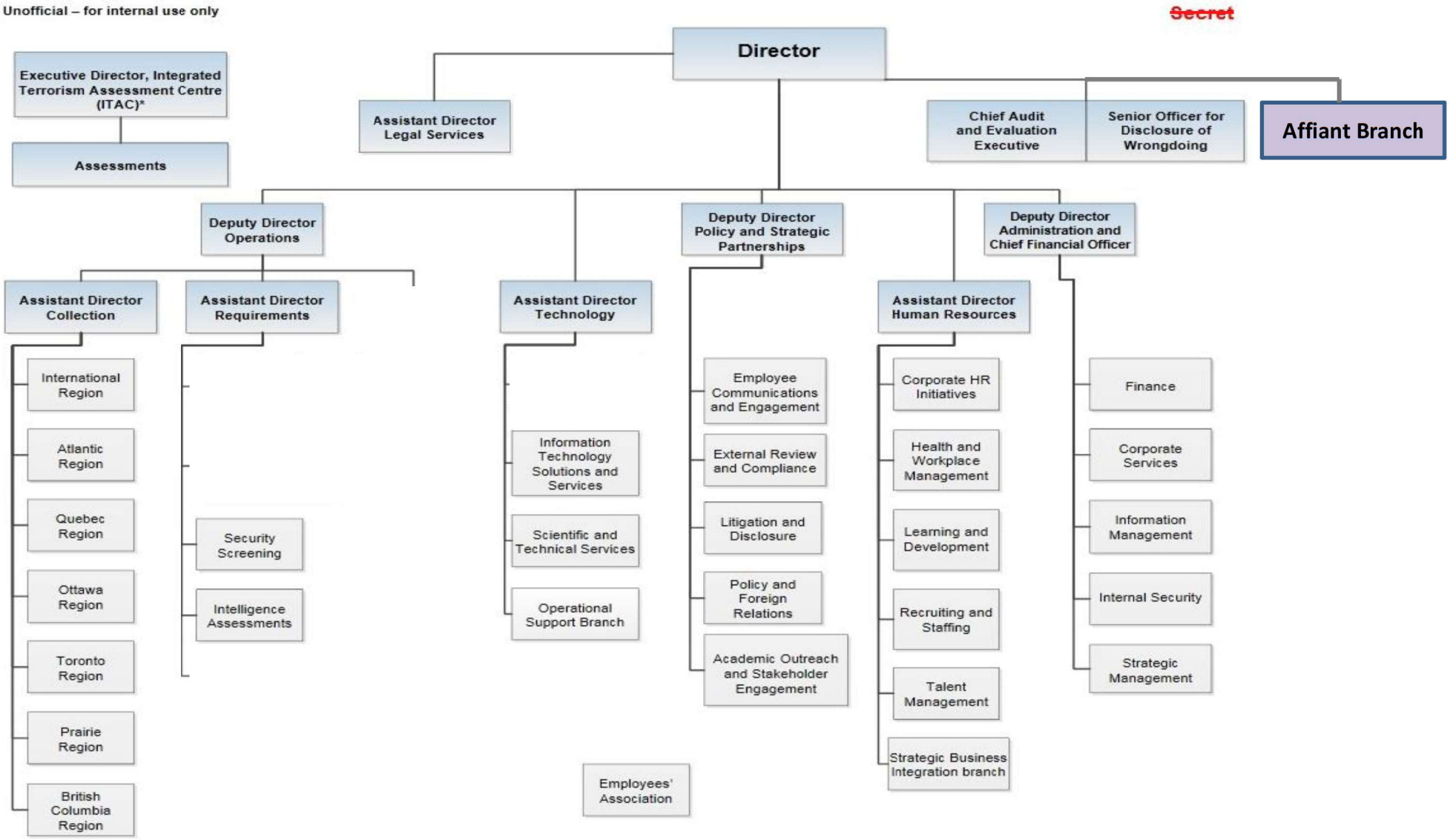


ANNEX C: Affiant Unit Organizational Structure



* ITAC is an interdepartmental unit in CSIS.

Recommended Affiant Branch Organizational Structure



* ITAC is an interdepartmental unit in CSIS.