National Security and Intelligence Review Agency

Office de surveillance des activités en matière de sécurité nationale et de renseignement

TOP SECRET // CEO

SURVEY OF THE CANADIAN SECURITY INTELLIGENCE SERVICE'S TECHNICAL CAPABILITIES

(NSIRA REVIEW 2020-09)

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
Tel: 1-833 890-0293 Fax: 613 907-4445

Table of Contents

EXECUTIVE SUMMARY

(U). Canada's national security confronts an evolving threat landscape. Consequently, CSIS must develop and acquire new, as well as adapt (repurpose) existing, technical capabilities in the course of its intelligence collection. This process presents potential compliance risk, as existing governance and legal frameworks may not capture the deployment of a capability, or CSIS personnel and supporting counsel may not understand how deployments are covered. These risks require NSIRA to maintain up-to-date knowledge of CSIS's full range of technical capabilities and related warrant powers.

(U). This survey offers a first step in this endeavor by surveying CSIS's suite of capabilities, along with its associated governance structure, and identifying areas of interest or concern to which NSIRA may return in future reviews.

(U). NSIRA reviewed information received in the form of briefings, written responses, and documents. The full range of technical capabilities CSIS currently employs in support of its intelligence collection operations was examined. NSIRA reviewed relevant policy and legal frameworks as communicated by CSIS, but did not conduct independent verification or audit of the claims or activities themselves.

(TS). The three primary groups implicated in the deployment of technical capabilities in support of operations are Operational (Ops) desks, Scientific and Technological Services (STS), and the Department of Justice (Justice). Ops desks turn to technical capabilities to fill gaps and corroborate information within their investigations. STS supplies and supports these capabilities, while Justice provides legal advice regarding proposed operations and offers the legal support to obtain the requisite Federal Court warrant(s) necessary to allow the operation to be undertaken.

(TS). The main policy suite related to the use of technical capabilities is outdated, by CSIS's own admission, and under revision, though the timeline for completing this task is unclear. In the interim, it is buttressed by *ad hoc* directives from senior leadership and other relevant policies and practices.

(TS). The framework by which CSIS assesses compliance and risk in this area is in a state of transition. Between winter 2018 and early 2021, the responsibility for ensuring technologies deployed in support of operations complied with CSIS's authorities rested with CSIS's [redacted] unit, initially created within the Deputy Director of Operations (DDO) Secretariat and subsequently housed under the Human Sources and Operational Support (HSOS) branch. The [redacted] unit was disbanded in 2021 (i.e. during the course of this survey). CSIS indicated its belief that greater efficiencies in addressing stakeholder needs and compliance gaps could be achieved through the division of [redacted] responsibilities amongst other units within HSOS branch, External Review and Compliance (ERC) branch, and STS, and is currently working on a transition plan to divide the [redacted] unit's functions between these three entities.

(TS). There is a risk that the division of these responsibilities may lead to "siloing" of information across different units and regions, a situation that could lead to compliance breaches. The [redacted] itself was created in the wake of an internal assessment made as part of [redacted], which had sought to address the decentralized compliance management issues that had contributed to compliance issues in the past. The dissolving of the [redacted] unit therefore presents NSIRA with an opportunity to review: (1) how CSIS divided the unit's compliance functions and (2) the effectiveness of the newly created system in assuring compliance.

(TS). Inaugurated in May 2021, the Operational Technology Review Committee (OTRC) is comprised of Justice counsel, technical experts, compliance officers, and warrant acquisition personnel. The committee's objective is to review: (1) all new technologies used to collect intelligence and (2) existing technologies that will be used in a new/different manner to collect intelligence. The creation of the OTRC suggests a positive step towards mitigating the risk of compliance breaches related to the deployment of technologies in support of operations. Most obviously, it presents a forum in which potential risks can be proactively identified and mitigated

(TS). A technical specialist drawn from STS, the [redacted] traditionally acted as a technical liaison between Ops desks and STS Policy Centres. In this role, [redacted] served as an information conduit between investigative teams, Justice and STS. In early 2021, CSIS senior leadership expanded [redacted] operational activities by engaging them in the Warrant Acquisition Process (WAP). The integration of the [redacted] into the WAP would seem to be a positive step towards mitigating some of the communication and knowledge gaps that contributed to compliance issues in the past.

(TS). Operational and support personnel, including STS, are required to take courses which aim to provide CSIS personnel implicated in the warranted operations with a foundational understanding of: (1) warrants and (2) the wider legal framework within which CSIS operates. Likewise, STS provides briefings to Justice about new technologies and is currently working with CSIS's Learning and Development branch to include material in the introductory course given to new Justice counsel. More broadly, STS also provides [redacted] presentations to Ops desk staff as part of their CSIS induction. While these initiatives have and will go some way to ensuring implicated personnel will have foundational knowledge of all aspects of the deployment of capabilities in the support of warranted operations, their long term efficacy is less certain, as it is relatively uncommon for refresher training to be undertaken.

(TS). CSIS acquires new technical capabilities in [redacted] ways: [redacted] Partnerships allow CSIS to realise and benefit from efficiencies created through the pooling of financial and human resources to develop solutions to shared technical problems and the joint identification of future technical and operational challenges. In a number of instances, CSIS is able to fill identified capability gaps by [redacted] technologies [redacted]

(TS). Each of CSIS's warranted technical collection operations are linked to one or more specific warrant types which, once issued by the Federal Court, provide the legal authorization for the

operational activity. Before a newly [redacted] developed technology is approved for operations, it undergoes testing to ensure: (1) that it is fit for purpose and (2) that it is compliant with the authorities under which CSIS operates. Finally, Section 3 of the *Ministerial Direction to the Canadian Security Intelligence Service: Accountability* (10 September 2019) requires CSIS to inform the Minister of Public Safety of operational activities in which "a novel authority, technique or technology, is used".

(TS). Special operations may include technical and traditional collection methods, which may be warranted or non-warranted. Specific operations may require multiple warranted authorizations depending on the intelligence collection method they employ. Operations are broadly categorized as involving [redacted]

(TS). Technical capabilities help facilitate the collection that occurs in these operations. These capabilities include those associated with the identification and survey of target devices, [redacted] Each capability, in turn, is composed of one or more underlying technologies [redacted]

(TS). Questions exist with regard to the robustness of CSIS's performance metrics program when it comes to technologies deployed in support of operations. In particular: (1) how CSIS assesses the operational effectiveness of the technologies it deploys; (2) the factors that inform CSIS's decisions regarding the allocation of scarce technological and expert personnel resources in the support of operations; and, (3) the foundations on which decisions are made to continue deploying an existing technology, invest in its modernisation, or replace it. CSIS needs to strengthen its performance metrics program with regard to its deployment of technologies in support of operations. The existence of a robust performance metrics program will be key to ensuring CSIS's effective use of its technology suite and expert personnel in operations.

(U). With respect to possible future NSIRA review, seven observations emerge.

(TS). First, there are potential risks associated with CSIS's outdated policy suite governing the deployment of capabilities in support of operations. The lack of current policies may result in heightened compliance risks, an issue of interest to future NSIRA reviews.

(TS). Second, the general state of flux and transition with respect to how compliance is monitored will be of interest moving forward. The main compliance unit – [redacted] – was disbanded in the course of the present survey, with its functions and responsibilities set to be distributed amongst existing entities within CSIS. Particularly given the [redacted] itself was created in response to previous compliance concerns, its dissolution suggests additional questions in this area that NSIRA may wish to consider in the future.

(TS). Third, CSIS's use of [redacted] technology and services may warrant targeted review. Relying on [redacted] technical capabilities introduces vulnerabilities and risks associated with exploitation that underscore the importance of rigorous security and compliance procedures. The use of partner technology presents further considerations, including the extent to which CSIS

leverages or depends on those partners [redacted]

(TS). Fourth, how CSIS monitors operational value has direct implications on the overall governance of technical capabilities in support of operations. A performance measurement regime is currently under development. Once in place, it will become an important feature of the governance framework, with attendant compliance implications for possible future NSIRA reviews.

(TS). Fifth, monitoring may be particularly important with respect to legal compliance vis-à-vis warranted and non-warranted activities. Tracking warrant details within operations could mitigate potential compliance risk in this regard. NSIRA is well-positioned to consider the issue in the future, with an eye toward explicit recommendations, particularly if coupled with an assessment of documented operational non-compliance incidents.

(TS). Sixth, some warrant-related compliance concerns are introduced by the interception and/or exploitation of information from devices not belonging to the target. To this end, NSIRA may wish to review a targeted subset of technical collection capabilities that present particular and pressing compliance risks.

(TS). Finally, seventh, it will be important for NSIRA to remain up-to-date with respect to technical aspects of CSIS special operations. Section 3 of the *Ministerial Direction to the Canadian Security Intelligence Service: Accountability* (10 September 2019) requires CSIS to inform the Minister of Public Safety of operational activities in which "a novel authority, technique or technology is used". These notifications could provide NSIRA with ongoing and up-to-date knowledge of CSIS's capability suite and how/when technologies are deployed operationally.

In recognition of continued transparency efforts with the Federal Court, NSIRA recommends that:

(U) Recommendation no. 1: The full, unredacted version of this report be shared with the designated judges of the Federal Court.

List of Acronyms

ADT - Assistant Director Technology

[redacted]

CSIS - Canadian Security Intelligence Service

DDO - Deputy Director Operations

ERC - External Review and Compliance

FY - Fiscal Year

[redacted]

HUMINT - Human Intelligence

HSOS - Human Sources and Operational Support

HQ - Headquarters

[redacted]

KPI - Key Performance Indicators

[redacted]

OE - Operations Enablement

OTRC - Operational Technology Review Committee

OPC - Operational Policy Center

Ops desk - Operational desk

[redacted]

RIS - Request for Investigative Support

[redacted]

SOP - Standard Operating Procedures

[redacted]

STS - Scientific and Technological Services

[redacted]

WAP - Warrant Acquisition Process

[redacted]

Definitions

Capability. Anything that enables CSIS to conduct operations. Capabilities are comprised of technologies and techniques. In some cases, more than one technology or technique can produce a capability.

Technique. A way of carrying out a particular task or operation.

Technology. Equipment (both hardware and software) developed from the application of scientific knowledge.

AUTHORITY

1. (U). This review is being conducted under paragraph 8(1)(a) of the *National Security and Intelligence Review Agency Act* (*NSIRA Act*).

INTRODUCTION

Background

2. (U). Canada's national security confronts an evolving threat landscape. Technological advancements combine with ongoing social, economic, and environmental change to ensure that new threats are added to old, and that both manifest in increasingly complex ways.[1] As a consequence, CSIS must develop and acquire new, as well as adapt (repurpose) existing, capabilities in order to effectively fulfil its mandate.

3. (U). Changes in technology present CSIS with a variety of new investigative opportunities. The data-rich environment of the modern world, for example, presents enormous amounts of information that can be gathered and processed into potentially valuable intelligence products.[2]

4. (TS). At the same time, the rapid rate of technological progress presents the risk that the policy and legal frameworks governing CSIS's operations cannot keep pace with technological advancements. As a result, there is a risk that CSIS's existing governance and legal frameworks may not capture the deployment of a new, or the novel use of an existing, capability. Likewise, CSIS personnel and supporting counsel may not understand how a new capability is covered by existing legal and governance frameworks. This lack of understanding means that CSIS may not have the legal and policy framework required to

---

[1] Camino Kavanagh, "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?" Carnegie Institute for International Peace, https://carnegieendowment.org (accessed September 23, 2020); Canadian Association for Security and Intelligence Studies (CASIS), "The Future of Canada Intelligence: Highlights from the CASIS Annual Symposium – November 8, 2019", https://casis-acers.ca (accessed April 12, 2021); Lindsay R. Sheppard et al., "The Spectrum of Encryption: Safety and Security Considerations", Centre for Strategic and International Studies, https://www.csis.org (accessed October 14, 2020); Aaron Shull et al., *Governing Cyberspace during a Crisis in Trust*, https://cigionline.org (accessed September 25, 2020) and Wesley Wark and Aaron Shull, eds., *Security, Intelligence, and the Global Heath Crisis: A CIGI Essay Series*, https://cigionline.org (accessed September 23, 2020).

[2] Canadian Security Intelligence Service, *CSIS Public Report 2019* (Ottawa: Government of Canada, 2020): 32; Brian Katz, "The Intelligence Edge: Opportunities and Challenges from Emerging Technologies for U.S. Intelligence", Centre for Strategic and International Studies, https://csis.org (accessed August 1, 2020); Katz, "The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection", Centre for Strategic and International Studies, https://csis.org (accessed August 1, 2020); and Katz, "The Analytic Edge: Leveraging Emerging Technologies to Transform Intelligence Analysis", Centre for Strategic and International Studies, https://csis.org (accessed October 14, 2020).

support the deployment of a new capability,[3] creating compliance risk. This possibility is not theoretical. NSIRA's 2018 review of CSIS's use of the [redacted] geolocation tool, for example, found that the lack of "developed policies and procedures around the assessment of new and emerging collections technologies," directly contributed to the risk that CSIS had breached section 8 of the *Canadian Charter of Rights and Freedoms* while trialing the tool.[4]

5. (U). Notwithstanding the challenges presented by the rapidly evolving technological environment, the Federal Court has stated that technological change "is no excuse [for CSIS] to flout or stretch [the] legal parameters [within which it conducts its activities]."[5]

6. (U). The compliance risks posed by CSIS's adoption of new and upgrading of current technologies, as well as its use of existing technologies in novel ways, requires NSIRA to maintain up-to-date knowledge of CSIS's full range of technical capabilities and related warrant powers. This survey offers a first step in this endeavor by surveying CSIS's suite of capabilities, along with its associated governance structure, and identifying areas of interest or concern to which NSIRA may return in future reviews.

Methodology and Information Requirements

7. (U). NSIRA reviewed information received from CSIS in the form of briefings, written responses, and documents. The latter included policies, procedures, project reports, operational planning documents, correspondence, technical studies and relevant legal opinions.

8. (U). NSIRA examined the tripartite information/knowledge sharing and support nexus that exists between CSIS's operational branches, technological branches and CSIS's Department of Justice counsel with regard to the deployment of capabilities in support of operations.

9. (U). NSIRA surveyed the full range of technical capabilities CSIS currently employs in support of its intelligence collection operations. NSIRA reviewed the training CSIS personnel received with regard to these capabilities and the policies that guide CSIS's deployment of technical capabilities. NSIRA reviewed relevant policy and legal frameworks as communicated by CSIS, but did not conduct independent verification or audit of the claims or activities themselves.

---

[3] Michael Nesbitt and Leah West, "Forum Introduction – Bill C-59, *An Act Respecting National Security Matters:* What It Does And Why It Matters", *Alberta Law Review* 57, 1 (2019): 172.

[4] See NSIRA, "Review of CSIS's Use of [redacted] – A Geolocation Data Collection Tool," (NSIRA Study 2018-05).

[5] *X (Re)* 2016 FC 1105 at para 262.

The Governance Framework

10. (U). The present section describes the overarching governance framework related to CSIS's capabilities, from the identification of a technical need (e.g. a gap in investigative capabilities) to the operationalization of a technical capability in the field. An understanding of this governance framework is necessary context for the survey of operations employing technical capabilities that follows. At the core of the section is a discussion of the relevant compliance and risk framework for technical activities. Given the nature of the present survey, however, compliance considerations are highlighted throughout, including those instances in which possible compliance risk is most acute and/or worthy of possible additional scrutiny, as well as other areas which may be of interest for future NSIRA review.

Key Players

11. (TS). Technical intelligence-gathering capabilities are crucial to CSIS's investigations. Intelligence gathered by technical capabilities facilitate and augment that obtained via CSIS's Human Intelligence (HUMINT) programs.[6] The three primary groups implicated in the deployment of technical capabilities in support of operations are Operational (Ops) desks, Scientific and Technological Services (STS), and the Department of Justice (Justice). Collectively described by CSIS as the "collaboration triangle", each group brings specialist and complementary skills and knowledge to the table that are integral to the execution of operations.

Figure 1: Technical Capabilities Deployment and Execution Collaboration Triangle

[6] [redacted] Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 23 February 2021.

12. (TS). As intelligence collectors, Ops desks turn to technical capabilities to fill gaps and corroborate information within their investigations (i.e. to obtain intelligence that they have been unable to acquire via HUMINT or other non-technical means such as physical surveillance). STS supplies and supports these capabilities, while Justice provides legal advice – including a legal risk analysis – regarding proposed operations andoffers the legal support to obtain the Federal Court warrant(s) required to allow the operation to be undertaken.[7] Operations requiring warrants enter the warrant acquisition process (WAP). Justice, as CSIS's legal counsel, is directly involved in this process.[8]

13. (TS). In order to have technical capabilities deployed in support of their investigations, Ops desks prepare and submit a Request for Investigative Support (RIS). A RIS is used to initiate or renew warranted and non-warranted special operations.[9] For warranted operations, each RIS is reviewed to ensure that the intended execution of warrant powers is authorized by the issued warrant, with ultimate approval required by designated approval authorities (EX level Chief or above). Once the RIS is approved, STS – in consultation with the Ops desks and other supporting branches such as [redacted][10] – prepares an operational plan designed to [redacted] This plan includes [redacted] Once the plan is conceptualised, it is sent to CSIS management (both regional and at National Headquarters [NHQ]) for review and approval.[11] Following execution, a post-operational report documents [redacted].[12]

14. (TS). The main policy suite related to the use of technical capabilities for operations is OPS-210.[13] First written in 2009, with updates to particular portions occurring through 2015, this policy suite is outdated by CSIS's own admission.[14] Although the suite is under revision, the

---

[7] Ibid.

[8] NSIRA is examining CSIS's warrant acquisition process as part of its review arising from the Federal Court's judgement in *2020 FC 616*. See NSIRA, "Press Release by National Security and Intelligence Review Agency on Federal Court En Banc Matter," http://nsirawet4.imatics.com/nwsspr/rlscmq/20200716-eng.html.

[9] [redacted]

[10] The [redacted] branch is responsible for providing support [redacted]

[11] [redacted] Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 23 February 2021.

[12] Ops-210: Execution of Warrant Powers and Non-warranted Special Operations (2009), [redacted]

[13] Ops-210: Execution of Warrant Powers and Non-warranted Special Operations (2009); [redacted]

[14] Email: CSIS to NSIRA "2021 05 17 - Tech Survey_OPS-210 policy."

timeline for completing this task is unclear. In the interim, OPS-210[15] is buttressed by *ad hoc* directives from senior leadership and more recent general policies and practices.[16]

15. (U). Notwithstanding the existence of *ad hoc* directives from senior leadership and other forms of guidance, the lack of an up-to-date policy suite – and therefore the possible reliance on obsolete policies – for the deployment of technical capabilities in support of operations presents a significant risk to compliance. This is an issue that NSIRA will consider when planning and conducting future technology reviews.

Compliance and Risk Entities

16. (TS). The framework by which CSIS assesses compliance and risk in this area is in a state of transition. Indeed, significant adjustments have occurred during the timeframe of the present survey. Below, several key entities and actors are discussed, along with the possible implications of recent developments for how compliance and risk will be monitored moving forward.

The [redacted] *Office* [redacted]

17. (TS). Between winter 2018 and early 2021, the responsibility for ensuring technologies and associated capabilities deployed in support of operations complied with CSIS's authorities rested with CSIS's [redacted] unit, initially created within the Deputy Director of Operations (DDO) Secretariat and subsequently housed under the Human Sources and Operational Support (HSOS) branch.[17] This responsibility was nested within the unit's wider mandate to "[a]ssure that highest levels of compliance with the law, warrants, ministerial direction, and policy in relation to all activities undertaken pursuant to section 21 [s.21] warrants."[18] In regards to technology, [redacted] responsibilities included:

- Communicating compliance-related requirements to STS and other technical branches responsible for the development and deployment of s. 21 collection and processing capabilities;
- Modernizing and maintaining related policies and procedures;
- Providing advice to CSIS's Operational Policy Centers (OPC) to aid, develop, and modernize standard operating procedures (SOPs) for individual technologies and techniques to help ensure compliance;

[15] During the factual accuracy phase of this review, CSIS stated that "The main policy used for technical collection was recently updated and published to CGS on 12 December 2021."
[16] "2021 05 13 - Supplementary questions via unclass email: Tech Survey."
[17] Human Sources and Operational Support (HSOS) is the CSIS headquarters branch responsible for the governance of CSIS' human source operations.
[18] CSIS, "Introduction to [redacted] - 20191021"; and, CSIS "[redacted] Vision-Mission-Functions".

- Providing policy advice and interpretation to regional/HQ STS units, regional/branch warrant coordinators and Ops desks;
- Conducting/supporting compliance accreditation of new systems/operational capabilities;
- Working with Justice to develop new warrant language for new technologies as required; and,
- Developing and maintaining [redacted] a definitive guide for CSIS personnel involved in the invocation and execution of warrant powers.[19]

18. (TS). The [redacted] unit was disbanded in 2021 (i.e. during the course of this survey). CSIS states that the decision was made to shutter the [redacted] unit after "[a] compliance framework review and an analysis of the business lines delegated to the Compliance group within [the External Review and Compliance (ERC) branch[20]] and the [redacted] group revealed that the areas of responsibility greatly overlapped without beneficial redundancy." CSIS further stated that internal consultations indicated greater efficiencies in addressing stakeholder needs and compliance gaps could be achieved through the division of [redacted] responsibilities amongst other units within HSOS, ERC, and STS, and is currently working on a transition plan to divide the [redacted] unit's functions between these three entities. This transition plan will involve the creation of a new group within STS.[21]

19. (TS). An in-depth examination of the [redacted] unit and its activities was not included in the scope of this survey. As such, NSIRA is unable to speak to how effective [redacted] had been in meeting its mandated responsibilities or whether the reasons provided by CSIS for its decision to disband the unit are sound. On paper, [redacted] was positioned to provide an important oversight function. It was also well situated to act as a communications and coordination hub between different groups within CSIS for: (1) policy development/modernization; (2) the standardization of procedures; (3) the ready transmission of compliance-related requirements as they evolve to the implicated parties throughout CSIS; and, (4) the sharing of lessons learned.[22]

20. (TS). Nor is NSIRA able to comment on the exact course CSIS intends to undertake to fill the gap created by the dissolution of the [redacted] unit, as the transition map was still being formulated at the time of writing. The fact that the transition plan was not completed prior to the abolishing of the unit, however, is of concern. There is a risk that the division of these responsibilities may lead to "siloing" of information across different units and regions, a

---

[19] CSIS, "[redacted] Description 2020-08-21"; and CSIS, "Introduction to [redacted] - 20191021".
[20] The External Review and Compliance (ERC) branch is the unit within CSIS responsible for providing support, coordination and communication on operational compliance.
[21] Email: CSIS to NSIRA, "2021 08 11 - Tech Survey_Former [redacted]-Transition," and Email: CSIS to NSIRA, "RE: 2021 08 11 - Tech Survey_Former [redacted]-Reason_for_folding."
[22] CSIS "[redacted] Description 2020-08-21"; and CSIS, "Introduction to [redacted] - 20191021".

situation that could lead to compliance breaches and that CSIS has experienced to its detriment in the past.[23] In 2016, in response to the Federal Court's *Associated Data* decision, CSIS stood up [redacted],[24] which reviewed issues of technical compliance and provided multiple recommendations to address these issues including the centralization of s. 21 compliance management functions within one unit. Indeed, the [redacted] was created in 2018 in response to this recommendation.[25] With the dissolution of the [redacted] unit and the division of its responsibilities amongst different groups, CSIS may be taking a step backwards as compliance management functions are once again being decentralized.

21. (U). The dissolving of the [redacted] unit presents NSIRA with an opportunity to review: (1) how CSIS divided the unit's functions; and (2) the effectiveness of the newly created system in assuring compliance.

The Operational Technology Review Committee (OTRC)

22. (TS). Inaugurated in May 2021 (i.e. during the course of the present survey),[26] OTRC is comprised of Justice counsel, technical experts, compliance officers, and warrant acquisition personnel (employees from outside these groups can also be invited to attend meetings as required[27]). The committee, which meets quarterly,[28] reports to the Assistant Director of Technology (ADT), and has the remit to review: (1) all new technologies used to collect intelligence; and (2) existing technologies that will be used in a new/different manner to collect intelligence.[29] The purpose of the committee's review is to:

- Identify any legal or privacy risks associated with the use of the technology;
- To identify potential mitigations to the legal or privacy risks identified;

---

[23] "CSIS's Warranted Collection of Information: [redacted] Operations," (SIRC Study 2016-02).
[24] In 2016 FC 1105, often referred to as the Associated Data decision, the Federal Court found that CSIS had unlawfully retained non-threat and third party information (associated data) that was linked to lawfully (warranted) collected communications. The Court was not made 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.
[25] CSIS, [redacted] CSIS, "Introduction to [redacted] - 20191021".
[26] The OTRC had been planned for at least one year before its launch. However, the COVID-19 pandemic caused repeated postponements of its first meeting. Email: CSIS to NSIRA, "2021 08 10 - Tech Survey_OTRC_background_info."
[27] During the factual accuracy phase of this review, CSIS has stated that additional members may include senior technical program managers and ERC or [redacted] personnel, although these are not explicitly listed in the OTRC Terms of Reference (TOR).
[28] Meetings can be called outside this cycle if required. CSIS, "OTRC TOR – Final Version"; and Email: CSIS to NSIRA, "2021 08 11 – Tech Survey_OTRC_final_ToR_meeting_minutes."
[29] CSIS, "OTRC TOR – Final Version"; and Email: CSIS to NSIRA, "2021 08 11 – Tech Survey_OTRC_final_ToR_meeting_minutes."

- To ensure that, if mitigations involve specifications to deployment of technology, these are incorporated in SOPs and employees receive training accordingly;

- To agree upon a standardized description of the technology to be used in a warrant application;

- To identify people who can act as technical affiant to explain this technology to the Federal Court, if required; and

- To identify novel technologies/collection processes that should be reported to the Minister of Public Safety under the 2019 *Ministerial Direction to the Canadian Security Intelligence Service: Accountability.*[30]

23. (TS). Technology is to be brought to the OTRC at the following times:

- When development of a new technology is initiated, or acquisition of a new technology is being considered;

- At the design (and/or design update) stage if information is different, or significantly more detailed, than that which was presented to the committee at the initiation phase; and,

- Prior to initial deployment of the new technology, to confirm there are no changes to the technology and the way it will be used, or to the legal environment, that would affect the original assessment by the committee.[31]

24. (S). The creation of the OTRC suggests a positive step towards mitigating the risk of compliance breaches related to the deployment of technologies in support of operations. Most obviously, it presents a forum in which potential risks can be proactively identified and addressed.[32] It will also assist in ensuring CSIS meets its obligations vis-à-vis both the Federal Court and the Minister of Public Safety to provide notice/briefings regarding the use of new technologies, or the novel use of existing technologies, in support of operations. Less obviously, by drawing together the different specialist groups within CSIS, the Committee has the potential to act as an important knowledge exchange and development hub between these different parties. Given the importance of these issues, NSIRA may wish to review the

---

[30] Section 3 of the *Ministerial Direction to the Canadian Security Intelligence Service: Accountability* (September 10, 2019) requires CSIS to inform the Minister of Public Safety and Emergency Preparedness of operational activities in which "a novel authority, technique or technology is used." See *Ministerial Direction to the Canadian Security Intelligence Service: Accountability*, https://www.publicsafety.ca (accessed 1 June 2021).
[31] Ibid.
[32] See for example the presentations made to the committee: CSIS, [redacted] Presentation for OTRC 2]"; CSIS, "[redacted] Presentation for OTRC –Final]"; and CSIS, [redacted] [OTRC_[redacted]]".

OTRC (whether narrowly or in the context of a wider review of the relevant internal compliance framework) to assess whether it is successfully meeting its mandate.

25. (U). In addition to supporting compliance and governance, the OTRC (along with the [redacted] – discussed below) has the potential to strengthen knowledge exchange and communication between the different groups within CSIS implicated in the development and deployment of technical capabilities.

The [redacted]

26. (S). A technical specialist drawn from STS, the [redacted] traditionally acted as a technical liaison between Ops desks and STS Policy Centres. In **this role,** [redacted] **served as an** information conduit between investigative teams, Justice and STS. In early 2021, CSIS **senior leadership expanded** [redacted] operational activities by engaging them in the WAP.[33] This decision was made because it was believed that the integration of [redacted] into the WAP would:

- Enable CSIS to use its collection capabilities to the greatest effect by identifying capability(ies) that "best fit" the objectives of individual operations;
- Provide better education for affiants and Justice counsel in the terms of technical knowledge (including direct access to subject matter experts when required); and,
- Proactively assist in compliance matters by ensuring that conditions/limitations discussed during the WAP are technologically achievable.[34]

27. (S). In addition to their WAP duties, [redacted] assist, as required, in:

- The identification and assessment of technology gaps and opportunities in order to improve ways that STS can aid investigations [redacted]; and,
- The research, evaluation and testing of new technologies in order to support the development and planning of operational capabilities and recommend future developments to maintain and improve intelligence gathering capabilities.[35]

[33] CSIS, "[redacted] Program Goals 2017/2018"; and "[redacted]". Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 23 February 2021.
[34] Email: CSIS to NSIRA, "2021 05 13 - Supplementary questions via unclass email: Tech Survey"; CSIS, [redacted]
[35] It is unclear how this responsibility relates to that of STS's Transfer to Operations branch (discussed below).

28. (U). [redacted] are based in NHQ and throughout CSIS's operational regions to provide onsite advice and support to investigative teams, as well as act as a communications conduit between STS personnel at NHQ and Ops desks.[36]

29. (U). The integration of the [redacted] into the WAP would seem to be a positive step towards mitigating some of the communication and knowledge gaps that contributed to compliance issues in the past. However, due to the recency of this change, the present survey was unable to assess the full impact of the arrangement on the drafting of warrants, CSIS's operational activities more generally, and knowledge sharing.

Knowledge Sharing and Training

30. (TS). As described above, STS, Ops desks, and Justice play integral, interrelated roles in the deployment of technology in support of operations. Each group provides specialist knowledge, skills, and expertise, without which operations would not be possible. However, in spite of the complementary roles that each of these groups play in support of the successful execution of operational activities, knowledge sharing and communications between them is not always optimal.[37] For example, different groups may have a limited understanding of factors involved in activities that exist outside their professional domain of expertise. Such knowledge gaps present a significant risk to compliance.

31. (TS). In a 2016 study of CSIS's [redacted] operations, for example, the Security Intelligence Review Committee (SIRC) found that instances of non-compliance had occurred because CSIS employees with expert knowledge of technologies had incomplete understanding of warrants, while those employees who understood the importance of warrant precepts had an imperfect understanding of technologies.[38] CSIS agreed with this observation and made a commitment to enhance staff training, as well as to provide briefings on new technologies to both Justice counsel and the Federal Court.[39] These commitments, along with the observations and recommendations made by the aforementioned [redacted] factored in the formation of the [redacted] (discussed above), as well as a variety of other initiatives in the fields of training and knowledge sharing. Importantly, these initiatives – some of which came online during this survey, and others which were slated to start in the last quarter of 2021[40] – indicate that CSIS recognises that training gaps and knowledge imparity between groups within the institution remains a potential compliance risk.

---

[36] CSIS, "[redacted] Program Goals 2017/2018"; and [redacted] Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 23 February 2021.

[37] See for example, "CSIS's Warranted Collection of Information: [redacted] Operations," (SIRC Study 2016-02).

[38] "CSIS's Warranted Collection of Information: [redacted] Operations," (SIRC Study 2016-02).

[39] Ibid.

[40] CSIS is currently establishing an annual workshop for operational employees to update them on new legal and policy developments. This workshop will include scenario-based training. The first workshop was to be held in fall of 2021. CSIS, *2020-21 Annual Report to the Minister on Operational Activities*, p. 60. See also comments regarding [redacted] and the Operational Technology Review Committee (OTRC), above.

32. (TS). For approximately the last two years, operational and support personnel, including STS, have been required to take the "Warrants 101" and "CSIS Legal Frameworks" courses. Designed and administered by the now defunct [redacted][41], these courses aim to provide CSIS personnel implicated in the warranted operations (acquisition, execution, and the analysis and retention of collected information) with a foundational understanding of: (1) warrants and (2) the wider legal framework within which CSIS operates.[42] Likewise, STS has not only begun to provide briefings to Justice about new technologies, but also is currently working with CSIS's Learning and Development branch to include material in the introductory course given to new Justice counsel. More broadly, STS also provides [redacted] presentations to Ops desk staff as part of their CSIS induction.[43] Finally, CSIS communicated that a newly created Training Unit within STS will "revisit" the training platform for special operations, and will manage technical training courses moving forward.[44]

33. (U). While these initiatives have and will go some way to ensuring implicated personnel will have foundational knowledge of all aspects of the deployment of capabilities in the support of warranted operations, their long term efficacy is less certain. Once the courses are completed, it is relatively uncommon for refresher training to be undertaken. As a result, personnel maintain and gain knowledge via other means, including: on-the-job osmosis, personal research, leveraging personal contacts for informal consultations/knowledge exchange, and via "trickle down effect" (i.e. information passed on to staff from management). The lack of formal continuing education and knowledge sharing/retention processes is of concern. In the fast-paced environment in which CSIS personnel operate, the possibility that such personal development will be sacrificed in favour of immediate operational needs seems significant. Moreover, the prevalence of CSIS's need-to-know culture can occasionally inhibit knowledge sharing. For example, since 2017 STS has provided detailed briefings to the Federal Court about new technologies or the use of existing technologies in novel ways.[45] Copies of the decks that support these briefings are not openly available to CSIS personnel, although they can be provided upon request.[46]

CSIS Technical Capabilities

34. (U). CSIS's technical capabilities, each comprised of one or more underlying technologies, help [redacted] activities and communications of individuals under investigation.[47] The present section provides an overview of how CSIS acquires and

[41] It is unknown which unit within CSIS will be responsible for administering the courses moving forward.
[42] Email: CSIS to NSIRA, "2021 05 13 - Supplementary questions via unclass email: Tech Survey".
[43] Email: CSIS to NSIRA, "2021 05 13 - Supplementary questions via unclass email: Tech Survey". See also CSIS, *2020-21 Annual Report to the Minister on Operational Activities*, p.60.
[44] Email: CSIS to NSIRA, "2021 05 13 - Supplementary questions via unclass email: Tech Survey".
[45] "CSIS Presentations/Technical Evidence Provided to the Federal Court – Post 2017". Information has also been provided to Minister of Public Safety since 2019. *Ministerial Direction to the Canadian Security Intelligence Service: Accountability*, https://www.publicsafety.ca (accessed 1 June 2021).
[46] E Mail: CSIS to NSIRA "2021 05 13 - Supplementary questions via unclass email: Tech Survey"
[47] [redacted] Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 23 February 2021.

evaluates the operational readiness of newly [redacted] developed technical capabilities, as well as a description of the special operations that employ them.

[redacted]

35. (S). CSIS acquires new technical capabilities to support operations in [redacted] ways: [redacted][49]

36. (S). The development of new capabilities is an expensive and often time-consuming endeavour requiring specialised skills. As such, CSIS frequently undertakes these activities with [redacted] partners. These partnerships allow CSIS (and its partners) to realise and benefit from efficiencies created through the pooling of financial and human resources to develop solutions to shared technical problems. They also enable effective horizon planning through the joint identification of future technical and operational challenges. Importantly, these partnerships allow CSIS to conduct research and access technologies that would otherwise be out of its reach, due to either cost or lack of expertise.[50] In the case of domestic partnerships, further financial efficiencies are often found through the aligning of strategic investments by coordinating [redacted]

37. (S). Despite the obvious advantages provided by these partnerships, challenges do exist. While presenting significant savings in development costs, and providing access to specialist expertise and experience that might otherwise be inaccessible, [redacted] partnerships are resource intensive, both financially and in terms of personnel commitments. Furthermore, in some instances it can be difficult for CSIS to find common ground with some of its [redacted] partners due to differences in: (1) levels of maturity between their technical programs; and, (2) authorities under which they operate. These challenges also exist with regard to [redacted] partners – such as the Royal Canadian Mounted Police and the Communications Security Establishment (CSE) – due to differences in mandate, authorities, and approaches.[52]

38. (S). In a number of instances, CSIS is able to fill identified capability gaps [redacted] This approach has a number of logistical advantages. As pre-existing technologies, [redacted] technologies are readily available and tend to be [redacted] than specialised technologies CSIS [redacted]

---

[48] [redacted]

[49] [redacted] Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 23 February 2021.

[50] Ibid. Also "CSIS – [redacted] Presentation". Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 25 February 2021.

[51] "CSIS – [redacted] Presentation". Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 25 February 2021.

[52] "CSIS – [redacted] Presentation". Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 25 February 2021.

[redacted] CSIS can also leverage [redacted] support for maintenance and repair. [redacted][53]

39. (U). In addition to [redacted] technologies to fill capability gaps, CSIS also [redacted] assist in the development of new capabilities. [redacted]

40. (U). As an illustration of the development process, CSIS highlighted to NSIRA [redacted] "future" technologies currently moving toward operationalization.[54] These technologies have the potential to extend some of CSIS's intelligence collection capabilities.

41. (TS). The [redacted] identified technologies were:

[redacted]

42. (TS). Before developed technology can be deployed, consideration must be given as to whether its use will, or will not, be covered by existing warrants and conditions. The above technologies-in-development help illustrate some of the possibilities in this regard. For example, [redacted] technology is related to [redacted] capability, but may be sufficiently distinct as to require a new warranted authorization.[55] [redacted] for their part, are [redacted] respectively (which are described in paragraphs 55 and 65, below), and are considered

[53] Email: CSIS to NSIRA "2021 08 05 - Tech Survey_Question_on_procuring_technologies."

[54] [redacted] Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 23 February 2021.

[55] This question was still being considered at the time of writing; regardless of the outcome in this particular instance, the key point is this type of assessment – covered or not? And, if not covered, a new warranted authorization may be required – occurs at this stage.

covered by established warrants and conditions employed in those contexts. If and how newly developed technology (and associated capabilities) will be covered will depend on the specific features and implications of the technology and the relevant terms and conditions of existing authorizations.

Ensuring Operational Readiness

43. (U). Each of CSIS's warranted technical collection operations (see paragraphs 51-69) are linked to one or more specific requested warrant powers. CSIS maintains templates for each category of warrant powers sought. CSIS edits these templates for each specific warrant application before the Federal Court.[56]

44. (S). Before a newly [redacted] developed technology is approved for operations, it undergoes testing to ensure: (1) that it is fit for purpose; and, (2) that it is compliant with the authorities under which CSIS operates. In the case of [redacted][57] tools and capabilities, STS's [redacted] group is responsible for planning and conducting these tests, as well as knowledge transfer to operational policy centres once a technology's operational readiness has been validated. [redacted] validates newly [redacted] developed technologies for compliance in three areas: (1) legal; (2) health and safety; and (3) regulatory[58]. In doing so, it consults with CSIS's operational policy centres to collect compliance requirements for operational scenarios. The purpose of this consultation is to allow [redacted] to ensure the technology is compliant with known warrant powers and conditions. STS does not have similar groups for [redacted] tools and capabilities.[59]

45. (S). In addition to conducting its own multi-step evaluation tests, STS also relies on [redacted] NSIRA notes that reliance on [redacted] presents a potential risk, insofar as CSIS remains ultimately responsible [redacted]

46. (S). [redacted] does not directly consult with Justice during the testing process, but rather relies on operational policy centres' input with regard to warrant powers and conditions. In fact, until the formation of the OTRC, no formal processes existed to ensure that legal opinions were

[56] Email, CSIS to NSIRA: "2020 12 29 - Response to Q1 (RFI dated 2020 12 09)_Review of Technology Employed by CSIS in Support of Operations"; CSIS, [redacted] - Terms (3.33 only)"; CSIS, [redacted] - Conditions (3.33 only)"; and CSIS, [redacted]

[57] [redacted]

[58] During the factual accuracy phase of this review, CSIS stated that "[redacted]

[59] [redacted]

sought from Justice before new technologies were developed, [redacted] and trialed. Rather, an informal consultation regime existed which saw STS approach Justice – either directly or indirectly – when STS leadership felt the need. While STS has conducted such consultations recently, it has not always done so.

47. (S). [redacted] reliance on the operational policy centres as a guide for its compliance activities is of concern. By CSIS's own admission, and as discussed above, many of its policy suites are outdated. Notwithstanding the buttressing of operational policy suites by senior leadership directives and general policies, practices and procedures, drawing on obsolescent policy suites to inform the compliance evaluations of new technologies presents a risk. Likewise, [redacted] reliance on the operational policy centres as a communications conduit between [redacted] and Justice is potentially problematic, as it presents the possibility of an inadvertent "broken telephone" effect in which both technical descriptions and legal advice can become garbled as it travels between groups. The newly established OTRC, described above, may go some way to mitigating this risk.

48. (S). NSIRA is also concerned that [redacted] main compliance activities appear to focus on health and safety and regulatory requirements, rather than legal and policy compliance. While NSIRA agrees that ensuring that newly [redacted] developed technologies are compliant with industry regulations and that health and safety requirements are met is important, placing primary focus on these areas presents a risk that legal and policy compliance may not receive the in-depth consideration they require. This, too, is an area in which the OTRC may help to mitigate risks.

49. (U). Finally, Section 3 of the *Ministerial Direction to the Canadian Security Intelligence Service: Accountability* (10 September 2019) requires CSIS to inform the Minister of Public Safety[60] of operational activities in which "a novel authority, technique or technology, is used". These notifications could aid NSIRA in maintaining up-to-date knowledge of both CSIS's capability suite, and how CSIS deploys technologies operationally.

Technical Capabilities Supporting Special Operations

50. (U). CSIS designates special operations as [redacted] Special operations may include technical and traditional (established human activities or procedures) collection methods, which may be warranted or non-warranted. Specific operations may require multiple warranted authorizations depending on the intelligence collection method they employ (e.g. a single operation may employ multiple

[60] Formerly the Minister of Public Safety and Emergency Preparedness; the portfolio was split following the 2021 federal election.

[61] Ops-210: Execution of Warrant Powers and Non-warranted Special Operations (2009), [redacted]

15(1)(d)
15(1)(f)
16(1)(b)

distinct technical capabilities, each of which may or may not require a specific warrant). [redacted] these operations fall into [redacted] broad categories:

[redacted]

51. (TS). Technical capabilities help facilitate the collection that occurs in these operations. These capabilities include those associated with the identification and survey of target devices (in support of special operations [redacted] The capabilities themselves are composed of one or more underlying technologies [redacted] Below, brief descriptions of current special operations – both warranted and non-warranted – provide further detail as to these capabilities and note, when applicable, relevant warrants as identified by CSIS.[63]

52. (TS). CSIS executes [redacted] operations to [redacted] operations are conducted without a warrant.

53. (TS). [redacted] operations are used to [redacted]

[62] [redacted] Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 23 February 2021.
[63] Unless otherwise noted, the source for this discussion of special operations (paragraphs 51-68) is [redacted] Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 23 February 2021.
[64] [redacted]

[redacted] The approach used to [redacted] is similar to that in [redacted] described above, [redacted] operations occur in the warranted and non-warranted spaces depending on the information captured by the equipment used.

54. (TS). In order to [redacted] operations are used to [redacted] operations are executed under the authority of a [redacted] warrant.

55. (TS). [redacted] operations provide CSIS with the ability to [redacted] operations are executed under the authority of a [redacted] warrant or a [redacted] warrant.

56. (TS). [redacted] operations, on the other hand, are used to [redacted] operations are executed under the authority of a [redacted] warrant.

57. (TS). In addition to [redacted] CSIS has the ability to [redacted] using a variety of different intelligence collection methods. [redacted] operations, for example, are used to [redacted] operations that [redacted] are conducted without a warrant. [redacted] operations that [redacted] are executed under the authority of a [redacted] warrant [redacted] or a [redacted] warrant for [redacted]

58. (TS). As opposed to [redacted] conducted pursuant to [redacted] operations, [redacted] operations are used to conduct [redacted] Capabilities developed in support of [redacted] operations can also be deployed to [redacted] operations are conducted without a warrant.

15(1)(d)
15(1)(f)
16(1)(b)

59. (TS). [redacted] operations are used for [redacted] are executed under the authority of a [redacted] warrant, but the establishment of [redacted] is conducted without a warrant.

60. (TS). [redacted] operations are used for the [redacted] and are executed under the authority of a [redacted] warrant. [redacted] operations, by contrast, are used when the same capabilities are deployed [redacted] and are conducted without a warrant.

61. (TS). [redacted] operations are used for the interception of [redacted] operations are executed under the authority of a [redacted] warrant for [redacted] warrant [redacted] warrant for [redacted] The resulting information includes [redacted] information.

62. (TS). [redacted] operations are used for the [redacted] This includes obtaining access to [redacted] This includes the collection of [redacted] operations are executed under the authority of one of [redacted] warrants: a [redacted] warrant [redacted] a [redacted] warrant [redacted] and/or a [redacted] warrant [redacted]

63. (TS). [redacted] operations can be used for [redacted] They are also used for [redacted] operations are executed under the authority of either [redacted] warrant [redacted] or a [redacted] warrant for [redacted]

[65] [redacted]

64. (TS). [redacted] operations are used to [redacted] The capabilities used to conduct [redacted] operations are predicated on CSIS' [redacted] These are typically obtained from [redacted] operations are executed under the authority of [redacted] warrant for the [redacted] or under the authority of [redacted] warrant for the [redacted]

65. (TS). In addition to its various methods of [redacted] CSIS uses technical capabilities to support [redacted] operations involve the search of [redacted] This could include [redacted] operations are executed under the authority of [redacted] warrant for [redacted] or under the authority of a [redacted] warrant for [redacted]

66. (TS). [redacted] operations are used for the collection [redacted] and are executed without a warrant[66].

67. (TS). [redacted] operations are used to [redacted] are generally accomplished by [redacted] While these [redacted] operations are conducted without a warrant, however, it was noted that [redacted] operations can be performed in parallel with [redacted] operations, namely during [redacted] In these cases, [redacted] to conduct [redacted] would be executed under the authority of a [redacted] warrant and [redacted] warrant respectively, and a [redacted] operation performed [redacted]

68. (TS). [redacted] operations are used for [redacted] This involves the [redacted] operations are executed under the authority of a [redacted] warrant for [redacted] or [redacted]

[66] [redacted]

15(1)(d)
15(1)(f)
16(1)(b)

69. (TS). Lastly, [redacted] operations are used for [redacted] which would be considered [redacted] operations. [redacted] operations are executed under the authority of one of [redacted] warrants depending on the information being sought: a [redacted] warrant [redacted] a [redacted] warrant [redacted] a [redacted] warrant [redacted] an [redacted] warrant [redacted] and/or an [redacted] warrant [redacted]

70. (TS). Over a sample period of 12 months, the deployment of special operations resulted in CSIS collecting approximately [redacted] of raw data, [redacted] To illustrate and contextualize the approximate volume of raw data collected, [redacted] would equal to [redacted]

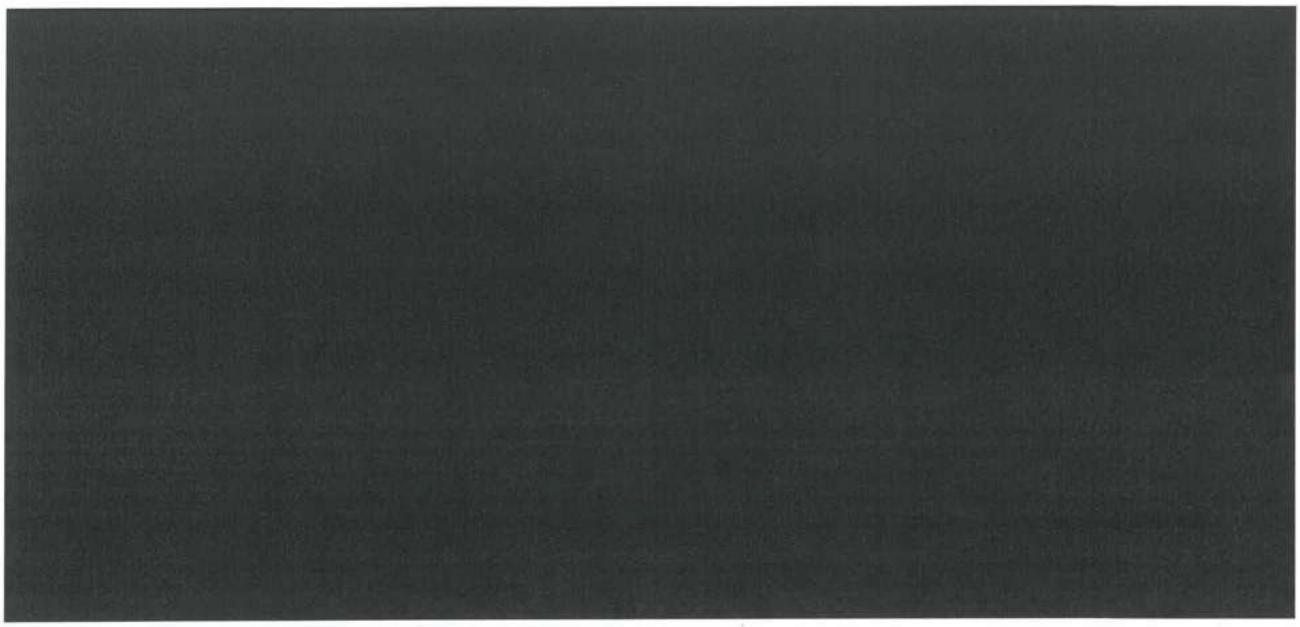
71. (TS). NSIRA received a special operations breakdown from CSIS that contained a list of all operations between 2018 and 2020.[69] Based on this report, STS initiated a total of [redacted] special operations between 2018 and 2021. Of these, [redacted] operations relied on warranted powers while [redacted] did not. Additionally, [redacted] While NSIRA was unable to verify the reason for this, [redacted] A detailed breakdown by special operation is provided in the table below:

[redacted]

[67] [redacted]

[68] [redacted]

[69] The information received in the RFI did not include data [redacted] operations.



72. (TS). Notably, STS does not retain any warrant details within the tracking of special operations aside from classifying them as warranted or non-warranted. The ability to associate the exact power within the warrant and its associated condition(s), [redacted] could lead to improved transparency when executing the power and respecting its conditions, [redacted] data and managing it, while minimizing the risk of operational non-compliance.

Tracking Operational Value

73. (S). STS tracks a number of Key Performance Indicators (KPIs) as part of the Assistant Director Technology's (ADT) Operations Enablement (OE) Performance Information Profile (PIP). These KPIs are intended to aid in the identification and assessment of: (1) training gaps and requirements; (2) resource reallocation requirements; and, (3) the impact of technologies on operations. An examination of OE PIP reports from mid fiscal year (FY) 2018-19 to mid FY 2020-21 suggests that these KPIs are of limited value. In a number of cases, results for years were not recorded and/or targets had not been determined.[71] This makes these reports at best imperfect tool for assessing the performance of some programs. The limited value of the OE PIP indicators in their current form is perhaps reflected by the fact that they are presently under review to assess their usefulness as an aid to ADT decision making.[72]

---

[70] [redacted]

[71] CSIS, "Mid-year 2020-21 OE Program Performance Report"; CSIS, "2020-21 Tear-End Performance Results – OE v2.0"

[72] Email: CSIS to NSIRA, 2021 03 11 - Tech Survey - Performance Metrics and Key Performance Indicators"; and Email: CSIS to NSIRA, "2021 08 10 - Tech Survey - PIP reports 2018 to 2021".

74. (U). STS programs also collect and track various types of performance data on technologies for its own purposes. It is not clear how this data is digested and deployed. STS has further indicated to NSIRA that it is planning to undertake an exercise to identify the best areas to track and measure performance to assess value. However, no concrete timeline for such an exercise exists. Nor is it is it known what shape that such an assessment will take, and how the information will be used.[73]

75. (U). Questions exist with regard to the robustness of CSIS's performance metrics program when it comes to technologies deployed in support of operations. In particular: (1) how CSIS assesses the operational effectiveness of the technologies it deploys; (2) the factors that inform CSIS's decisions regarding the allocation of scarce technological and expert personnel resources in the support of operations; and, (3) the foundations on which decisions are made to continue deploying an existing technology, invest in its modernisation, or replace it.

76. (U). NSIRA acknowledges that it can be difficult to assess and/or quantify the intelligence value of information gathered by individual technologies, for two main reasons. First, the data gathered by different technologies in support of an individual operation are amalgamated and processed (often multiple times) before being reviewed. In doing so, the information is transformed in such a way that makes the data's true provenance difficult to ascertain. Second, the diverse technologies deployed by CSIS when combined with the distinct character of operations can make comparison difficult, if not impossible.[74]

77. (U). These challenges recognised, the development of a robust performance measurement regime designed to measure accurately the frequency that individual technologies are deployed, and the impact these technologies have on investigations, is important. Such information would help CSIS to identify the relative investigative value of particular technologies it employs. This in turn would allow for: (1) informed decisions regarding the allocation of scarce technological and expert personnel resources towards areas where they can be most effective operationally; and (2) allow for the prioritisation of investments in technological renewal. This information will be of particular importance as the costs of maintaining technologies to support some capabilities become increasingly prohibitive.[75] More broadly, such a regime would enable CSIS to support its position that the current legislation governing its operations is, as CSIS leadership has argued, "set[ting]

---

[73] Email: CSIS to NSIRA, "2021 03 11 - Tech Survey - Performance Metrics and Key Performance Indicators."
[74] Ibid.
[75] [redacted] Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 23 February 2021; and, "CSIS – [redacted] Presentation". Briefing provided to NSIRA by CSIS's Scientific and Technical Services, 25 February 2021.

technological limitations on intelligence collection that...unduly limit [CSIS's] investigations."[76]

78. (TS). At the request of NSIRA, CSIS produced statistics detailing the type and frequency of approved technical operations and undertaken technical operations (with the latter a subset of the former) from 2018 to March 2021. By CSIS's own admission, this entailed a considerable amount of effort, as CSIS has not traditionally tabulated this information.[77] This is because CSIS's traditional statistical measurement with regard to the deployment of technology focusses on whether an operation fulfills an intelligence gap. CSIS further noted that the exercise was useful because it: (1) offered insight as to why approved operations did not materialise; and, (2) demonstrated the impact of external factors – such as COVID-19 and the implementation of Bill C-59 – on operations.[78] NSIRA notes that the tabulation of this information on a regular basis would offer CSIS considerable insight into the factors that cause approved operations to not be actioned [redacted] In turn, this information could inform operational planning, resource allocation, and highlight potential gaps/weaknesses in capabilities. Unfortunately, CSIS has indicated that the significant level of investment in time and resources required to tabulate and interrogate this data means that it is unlikely that this exercise will be undertaken on a regular basis.[79]

79. (U). CSIS needs to strengthen its performance metrics program with regard to its deployment of technologies in support of operations. The existence of a robust performance metrics program will be key to ensuring CSIS's effective use of its technology suite and expert personnel in operations. As such, NSIRA will continue to monitor the evolution of this program in future technology reviews. In particular, in the short term, NSIRA will be interested in seeing both the outcome of STS's exercise to identify the best areas to track and measure performance to assess value, and the conclusion that is reached with respect to the usefulness of the ADT's OE PIP report.

OBSERVATIONS

80. (TS). This survey provided NSIRA with foundational knowledge of CSIS's technical capabilities, including how they are acquired, the broad framework by which they are governed, and the extant intelligence collection operations in which they are used. With respect to possible future NSIRA review, seven observations emerge.

81. (TS). **First, there are potential risks – acknowledged by CSIS itself – associated with it's outdated policy suite governing the deployment of capabilities in support of operations.** The lack of current policies may result in heightened compliance risks, an issue of interest to future NSIRA reviews.

---

[76] David Vigneault, Director, CSIS, "National Security, Economic Prosperity and Canada's Future," Center for International Governance Innovation, February 9, 2021. Recording available at cigionline.org.
[77] Email: CSIS to NSIRA, "2021 04 16 - Tech Survey - Breakdown of Technical Operations."
[78] Email: CSIS to NSIRA, "2021 05 13 - Supplementary questions via unclass email: Tech Survey."
[79] Ibid.

82. (TS). **Second,** and relatedly, **the general state of flux and transition with respect to how compliance is monitored will be of interest moving forward.** The main compliance unit – the [redacted] – was disbanded in the course of the present survey, with its functions and responsibilities set to be distributed amongst existing entities within CSIS (including the ERC, NSIRA's main point of contact across all CSIS reviews). This is of interest both with respect to possible compliance reviews of specific CSIS activities (i.e. were/are internal compliance mechanisms sufficiently robust vis-à-vis said activity?) but also possible review of the new compliance framework itself (i.e. does the new system adequately address compliance risks?). Particularly given the [redacted] itself was created in response to previous compliance concerns – identified as part of [redacted] – its dissolution suggests additional questions in this area that NSIRA may wish to consider in the future.

83. (TS). **Third, CSIS's use of [redacted] may warrant targeted review.** [redacted] relying on [redacted] technical capabilities introduces vulnerabilities and risks [redacted] underscore the importance of rigorous security and compliance procedures. The use of partner technology presents further considerations, including the extent to which CSIS leverages or depends on those partners [redacted] Arrangements between CSIS and [redacted] partners with respect to technology and technical capabilities therefore presents fruitful terrain for future NSIRA review along a variety of dimensions.

84. (S). **Fourth, how CSIS monitors operational value has direct implications on the overall governance of technical capabilities in support of operations**. As noted above, a performance measurement regime is currently under development. Once in place, it will become an important feature of the governance framework, with attendant compliance implications for possible future NSIRA reviews.

85. (TS). **Fifth, monitoring may be particularly important with respect to legal compliance vis-à-vis warranted and non-warranted activities.** As indicated by Table 1 above, certain operations identified by CSIS as involving technical collection under specific warrants also reported non-warranted collection. Tracking warrant details within operations – i.e. which warranted power (and associated conditions) was used for which collection activity – could mitigate potential compliance risk in this regard. NSIRA, for its part, is well-positioned to consider the issue in the future, with an eye toward explicit recommendations, particularly if coupled with an assessment of documented operational non-compliance incidents. Such a review would aim to identify, diagnose and possibly eliminate residual risk associated with the invocation and execution of warrants, the associated technical capabilities, and the special operations that enable intelligence collection.

86. (TS) **Sixth, some warrant-related compliance concerns are introduced by [redacted] information from devices** [redacted]

[redacted] To this end, NSIRA may wish to review a targeted subset of technical collection capabilities that present particular and pressing compliance risks.

87. (U). Finally, **seventh, and most broadly, it will be important for NSIRA to remain up-to-date with respect to the technical aspects of CSIS intelligence collection operations, particularly given the speed with which technology and associated technical capabilities change and evolve.** As part of this effort, it may be possible to leverage existing reporting requirements already undertaken by CSIS. For example, Section 3 of the *Ministerial Direction to the Canadian Security Intelligence Service: Accountability* (10 September 2019) requires CSIS to inform the Minister of Public Safety of operational activities in which "a novel authority, technique or technology is used". These notifications could provide NSIRA with ongoing and up-to-date knowledge of CSIS's capability suite and how/when technologies are deployed operationally. Because CSIS already produces such notifications, doing so would not impose additional resource burdens, but merely leverage existing work for mutual institutional advantage. Given the possible compliance implications of introducing novel techniques and technologies (as described in this report), NSIRA will have an ongoing interest in these cases. The notifications could improve review planning and accelerate the initiation of specific reviews by providing a baseline of information. At the same time, regular sharing of the notifications would alleviate resource burdens on CSIS associated with *ad hoc* and potentially wider-ranging requests for information, with such requests reserved for instances in which NSIRA has already identified a specific activity or operation of interest. Further, the sharing of the notifications would bolster CSIS's efforts toward proactive transparency, in line with, for example, commitments to provide explanatory briefings to the Federal Court on new technologies used in warranted operations.

In recognition of continued transparency efforts with the Federal Court, NSIRA recommends that:

(U) Recommendation no. 1: The full, unredacted version of this report be shared with the designated judges of the Federal Court.