Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

TOP SECRET // CEO

SIRC REVIEW 2016-02
CSIS'S WARRANTED COLLECTION OF INFORMATION: OPERATIONS

SUMMARY

Last year, SIRC's review of operations examined CSIS's compliance with applicable warrants, as well as the processes it had in place to support compliance with warrants. The present review continued this focus on CSIS's use of warrant powers.

The review's overarching objective was to assess the processes in place at CSIS to ensure its compliance with the terms and conditions of the applicable warrants. The review focussed on the execution of warrant powers in three specific contexts. One area of focus was a specific type of operation, . The second area involved a series of warrant non-compliance incidents that occurred for intermittent periods since March 2012. These incidents of non-compliance were reported to the Federal Court during its *en banc* process beginning in December 2015. Finally, the review also examined a specific operation which occurred absent legal authority.

The review identified several areas of risk with respect to compliance with warrants, including that the flow of information between those responsible for providing legal advice and those responsible for the execution of warrants could be enhanced. The review resulted in a number of findings and recommendations intended to diminish those risks in the future. To that end, overall, this review emphasized the need for training for those with warrant-related responsibilities, the utility of centres of excellence with respect to the execution of warrants and the ongoing requirement to seek legal advice when there is any doubt with respect to warrant authorities.

File No. 2800-206

ATIP version
dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Table of Contents

ATIP version
FEB 2 5 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

1 INTRODUCTION

Last year, SIRC's review of operations examined CSIS's compliance with the applicable warrants, as well as the processes it had in place to support compliance with warrants. The present review continued this focus on the execution of warrant powers in three specific contexts.

The first area of inquiry focused on one specific type of operation, . The second involved a series of warrant non-compliance incidents that occurred for intermittent periods since March 2012; at the time SIRC was briefed on these incidence, they had been attributed largely to actions taken by and to issues related to the technology used to process intercepts. Finally, during last year's review of close access activities, CSIS informed SIRC of an intercept operation which occurred absent legal authority from the Federal Court.

CSIS acknowledges that the proper execution of warrants is of utmost importance. At the time of writing, CSIS is in the midst of a business modernization process that aims to, inter alia, reform warrant-related processes to ensure the highest level of assurance of compliance with warrant conditions and policy requirements.

Throughout this review, SIRC was mindful of CSIS's own ongoing process of review of warrant-related issues, the results of which are anticipated in fall 2016. SIRC identified several recurring themes that may provide fodder for this exercise. This review emphasizes the need for training for those with warrant-related responsibilities, the utility of centres of excellence with respect to the execution of warrants and the ongoing requirement to seek legal advice when there is any doubt with respect to warrant authorities.

ATIP version
dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

2 METHODOLOGY

SIRC's research focused broadly on how CSIS ensures compliance with the terms and conditions of warrants. In each section, there were more specific questions guiding the review, including: what are the key challenges confronting CSIS in the area of operations; how has technology affected the role of the and to what extent is technology responsible for the retention errors that occurred; and what were the factors that led to the non-compliance issue that occurred in

A primary focus was to assess whether CSIS's execution of its powers complied with the parameters of the warrant(s) cited as authority for the operation. The review also examined CSIS's compliance with the *CSIS Act*, in particular by evaluating whether the use of any of CSIS's powers was "unreasonable" or "unnecessary." In addition, the review assessed whether CSIS observed the standards of good governance.

SIRC assessed a sample of operations for compliance with the relevant warrant authorities. There was a substantial regional component, both through the sample work that touched on each region, as well as through visits/video-conferences and exchanges with each region to discuss the work of

SIRC met with CSIS representatives on multiple occasions to provide context to the issues under review. The discussions included meetings with CSIS representatives from the Branch, , heads, operational desks, managers, the Department of Justice, National Security Litigation and Advisory Group (NSLAG), from HQ and the regions, as well as select working groups. SIRC's understanding of the technical elements of these operations benefited from those meetings. SIRC also received briefings on a number of retention/non-compliance issues, which will be addressed later in the report.

ATIP version
dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

3

3.1

ATIP version
dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

3.2

ATIP version
dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

3.3 Due Diligence

Given the risk to the privacy SIRC examined the processes underpinning CSIS's . This involved a review of Requests for Investigative Support (RIS), on the basis of which an approval for the execution of a warrant power is sought, as well as the associated operational plans for a sample of operations.[10] SIRC observed that information and justifications were not always included in the RIS or operational plan. As a result, it was not straightforward for SIRC, in many cases, to assess the basis on which Similarly, neither would it have been straightforward for those responsible for approving the operations to adequately assess the justifications. This is problematic given the need to . On this, CSIS affirmed that it is "unreasonable to assume that "[11] Outside of the RIS process, however, **SIRC found that the regions, in concert with HQ, did make efforts to**

ATIP version
dated: FEB 2 5 2019

[10] The sample consisted of operations that occurred during the review period. The sample included operations from all regions.
[11] Email exchange, "RE: " 11 June 2014

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

SIRC's observations with respect to the RIS process were raised by in 2014. In particular, raised concerns to HQ about issuing generically worded RISs

SIRC is aware that, even earlier, in 2013, concerns were raised by

It was explained to SIRC that since 2009, CSIS has instituted a process for operations

SIRC acknowledges this as part of CSIS's due diligence with respect to the execution of this warrant power, along with the main elements of the RIS process.

Notwithstanding that, **SIRC found that it was problematic that information and the justification were not included in the RIS.** It is the RIS that is intended to verify that the proposed operation is authorized by a warrant and that the proposed operation adheres to any conditions imposed therein. The Warrant, cited as the authority for the operations, typically authorizes CSIS to obtain information and to execute the warrant . SIRC's concern is that a process for is an important exercise of due diligence. As a result, **SIRC found that not including information in the RIS, and information justifying created a risk of non-compliance with the warrant.** SIRC additionally observed that the concerns raised by the two regions were not adequately addressed in that the Department of Justice, National Security Litigation and Advisory Group (NSLAG) was not consulted to ascertain the amount of due diligence required to execute this warrant power.

In June 2015, HQ drafted new standard operating procedures (SOPs) for operations. The SOPs include a requirement to include in the RIS the reason to believe

In this way, **SIRC found that the new SOPs with respect to the RIS reflect the requirement to**

ATIP version
dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

3.4 Legal Authorities

On a broader level, rapid changes in technology also brought about a rethink of the warrants CSIS was using, particularly the Warrant.

The framework of the relevant part of the Warrant, read as a whole, captures the early operations Over the life of CSIS's operations, however, there was a significant change in the focus of the warrant execution

In 2015, a new warrant was created - the Warrant. This warrant type brings together most operations including operations. The Warrant reflects the current reality of CSIS' operational environment A review of the template of this warrant reveals provisions specifically authorizing CSIS to

ATIP version
FEB 2 5 2019
dated:

In SIRC's view, the warrant did not contemplate the eventual focus of operations Although this was eventually changed with the new warrant, SIRC believes that consultations with NSLAG should have occurred once the focus of operations shifted . This would

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

have provided an opportunity to mitigate any risk that the specifics of the operation had exceeded what was allowable under the warrant authority. Although SIRC is aware that formal and informal consultations did take place with NSLAG in the context of specific operations, SIRC was provided no evidence of any broader consultations with NSLAG on the changing orientation of operations before those triggered by the legislative amendments pursuant to the *Protection of Canada from Terrorists Act.*

SIRC is aware that, HQ's provided guidance on warrants as a regular practice and had a standing authority to consult NSLAG as necessary on individual warrants. This practice changed in spring 2015 Now, the regions are encouraged to seek legal advice as necessary, for the proper execution of warrants. Alongside this, there should be an on-going flow of information between NSLAG and CSIS on the technical details related to the execution of warrant powers.

ATIP version
dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

4 RETENTION OF INFORMATION COLLECTED UNDER WARRANT

There are computer systems that help process intercepted communications.

4.1 Warrant Non-Compliance

Starting in March 2016, CSIS implemented new audit requirements to confirm that systems were compliant with the retention policies and warrant conditions. As a result of this new process, CSIS learned that for intermittent periods since March 2012,

ATIP version
dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

information had been retained in excess of the warrant conditions. In total, four separate categories of errors were initially identified: 1) technological failures 2) technological failures 3) processing errors; and 4) failures. Taken as whole, these events constitute one of the Service's most significant instances of warrant non-compliance. Given the seriousness of this issue, CSIS working groups were established to complete a full analysis on the scope and impact of this discovery, and external stakeholders were also informed – including the Minister, Federal Court and SIRC.[21]

The technological errors and processing errors are examined below, while failures will be reviewed within SIRC's upcoming study.[22]

4.1.1 Technological Errors & Processing Errors

CSIS determined that an automated alert ceased to function,

The CSIS working groups noted that some information which had been flagged for future review was found to have been maintained beyond the retention period; in other words, employees failed to go back to ensure warrant compliance. Moreover, some employees had also occasionally misidentified the type of report they had written resulting in information being retained in excess of warrant conditions. According to CSIS's analysis, these errors affected less than one percent of sessions during this time period.[24]

---

[21] The Federal Court was first advised of this issue on April 29, 2016, and sent a report on June 7, 2016. The Minister of Public Safety was verbally informed on May 2, 2016 and sent a report on May 25, 2016. Finally, SIRC was provided with a detailed briefing on May 6, 2016 and again on August 15, 2016.

[22] As the CSIS working groups continued their analysis over summer 2016, additional retention problems were identified.

This matter was investigated . While the process failure did not lead to a breach of warrant conditions *per se*, the resulting recommendations included a recommendation to advise the Court of the problem and Service efforts to rectify the situation."

[24] CSIS Memorandum, "The Retention and Destruction of Materials and Communications Obtained Under Warrant," June 3, 2016, p.8; and, Refer to CSIS Email, "Re: Responses to SIRC Questions form SIRC 2016 07 13 – ," July 20, 2016.

ATIP version dated: FEB 25 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

4.1.2 CSIS Assessment

CSIS believes that "although the retention issues resulted in significant instances of non-compliance, the actual impact on the privacy of individuals was minimal."[25] This conclusion was reached based on CSIS's assessment that the retained data was not used for operational reporting purposes and was not accessed by any parties other than those who are responsible for its reporting. SIRC closely reviewed efforts by CSIS to delete all of the improperly retained including following daily updates within the CSIS Branch responsible for this process.[26] CSIS has initiated additional machine alerts and new human auditing processes to reduce similar occurrences. Most critically, in SIRC's opinion, is CSIS's recently initiated which in light of the issues, is expected to establish an improved management system to govern the warranted collection and retention of information. Project findings are to be reported to the CSIS executive in the fall of 2016.[27]

4.2

Those responsible for debriefing, recording and flagging the information CSIS receives from its warranted collection into the above mentioned databases are the

. Accordingly, play an integral role in ensuring compliance with Federal Court warrants, the *CSIS Act* and operational policies/procedures.[28]

When making determinations about what information to retain within CSIS's databases,

29

Irrespective of the various reasons for the errors which are being assessed by SIRC identified three categories of concern particular to

---

[25] CSIS Memorandum, "The Retention and Destruction of Materials and Communications Obtained Under Warrant," June 3, 2016, p.10.
[26] As of June 6, 2016, CSIS confirmed that all of the initially identified errors had been deleted. Refer to CSIS file: and, SIRC meeting with team, August 15, 2016.
[27] Refer to DDO Memo, July 15, 2016; and, SIRC meeting with team, August 15, 2016.
[28] SIRC spoke to CSIS's as well as representatives from across all of CSISs regions in order to acquire context on intercepts.
[29] SIRC was told that in order to remain compliant with the "strictly necessary" aspect of the *CSIS Act*, the must use the justification(s)

ATIP version FEB 25 2019 dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

the program that require further clarification and attention: these include, technological, responsibilities and employee training.

Second, linked to previous technological limitations , are varying interpretations about responsibilities.

The question about who is best suited to perform certain tasks related to intercept products is complex.

. Indeed, SIRC was left with the overall impression that roles and responsibilities were increasing, yet working out who is to do what, and when, still required further precision. Fortunately, making such determinations is the ongoing preoccupation of CSIS's , which SIRC is concurrently examining.

The third and final observation is on the adequacy of training.

ATIP version
dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

In SIRC's opinion, the reason the errors had continued unnoticed for so long was, in part, due to the fact that those employees with expert knowledge of intercept technologies and CSIS databases had incomplete knowledge of warrants, while those employees who knew about the importance of warrant precepts had incomplete knowledge about the technologies used for collection and retention. As such, **SIRC found that a gap has slowly developed between CSIS's use of technology and the management of critical compliance functions.**

Ultimately, CSIS needs to ensure that the accountability structure for compliance with Federal Court warrants and internal policies is appropriately robust. Although work towards achieving consistency in national standards has been in progress for some time, the program, in particular, lacks a 'center of excellence' with adequate resources to spur necessary change.

Given that the rationale for selecting one organizational model over another may change over time, CSIS may wish to re-examine the location within the organizational structure for the

Overall, SIRC was impressed by the professionalism and dedication exhibited by They not only perform a difficult job , but additionally play a critical role in ensuring compliance with Federal Court warrants, the *CSIS Act* and operational policies/procedures. Indeed, the interplay between complex technology, legal requirements and competencies will be the subtext to the modifications CSIS will need to make to the program over the longer-term; how this is incrementally achieved will require considerable analysis. The are already seized with this holistic assessment, and SIRC will therefore revisit this important compliance responsibility in future reviews.

ATIP version
FEB 2 5 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

5 NON-COMPLIANCE

During last year's review of activities, CSIS informed SIRC of an intercept operation which was "non-compliant ."[37] Given that the incident involved activity, SIRC elected to follow-up within this study.

The non-compliance occurred , involving the use of within . This was the first use of by CSIS . Although documents revealed that there was some initial discussion between and HQ stakeholders on how this activity would be covered by the then-existing warrant(s), it was ultimately decided that the proposed operation should proceed.[38] Four months later, proposed to use , resulting in scrutiny similar to what had transpired within , with one important difference: contacted the office of the Deputy Director Operations (DDO), which then sought legal advice about the proposed activity.[39] Based on this advice, the operation did not proceed.[40]

HQ informed of the legal interpretation the same day it was provided and were immediately terminated.[41] It is important to note that NSLAG had first been solicited prior to the operation.[42] At that time, however, there was no single location for all legal opinions, and therefore, stakeholders were not uniformly aware of pertinent legal advice. This has since been rectified following CSIS's placement of all legal opinions within a single and accessible location; an initiative derived from a SIRC recommendation within Study 2015-01.

A number of observations can be made from the non-compliance and its aftermath. To begin, it is problematic that some employees in and HQ believed was permissible, while other employees in and HQ thought otherwise. Had not sought clarification, the operation would have continued. Moreover, confusion over warrant precepts was demonstrated earlier that year between and

---

[37] CSIS Email, " Non-compliance

[38] CSIS Email, "RE: Answers: // Warrant, Paragraphs,"

[39] CSIS Email, "FW:

[40] The legal advice noted the following:

". Refer to CSIS Email, "

[41] SIRC confirmed termination and also confirmed that the collected data was purged from all corporate and operational systems. Refer to CSIS Email, "RE: NOT to be invoked "

[42] Memo, "SIRC Study 2016-02, CSIS's Warranted Collection of Information: Operations," August 22, 2016.

ATIP version FEB 25 2019 dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

HQ, an incident covered in detail within SIRC Study 2015-01. Finally, the 2016 non-compliance incident(s) brings SIRC's growing concern on this subject into contemporary focus; namely, **warrant training for employees is not consistent across job functions.**

Ensuring warrant compliance can be unnecessarily complicated by the fact that certain employees are asked frequently to provide *de facto* legal advice in the context of warrant executions. This is particularly true of for example, who review Requests for Investigative Support.[43] CSIS has underscored both internally to employees, and externally to SIRC, on the importance of when questions about warrant advice is raised.[44] Despite the importance of this position for the execution of warrants, **SIRC found that CSIS has not created consistent standards for the hiring, training and job functions expected of**

It is not always possible, nor operationally expedient, for regions to seek formal legal advice. On a practical level, most questions can be addressed either at the regional level or through consult within HQ without having to consult formally or informally with the NSLAG. It is therefore important, that beyond ensuring all employees who are involved in the execution of warrants receive standardized training, that possess substantial warrant expertise. This would require that CSIS develop standardized performance expectations, and measurements for this cadre of employee.

Soon after the intercepts were terminated, CSIS instituted a number of additional practices to help ensure more visibility on ,[45] and the Minister of Public Safety was informed within the Director's 2014-2015 annual report. Finally, concern over a repeat of this error was rendered moot following changes to warrants in the spring of 2015 which permit the use of .[46] Given changes to the warrant regime allowing CSIS to perform an activity which had previously been executed in absence of legal authority to do so, SIRC enquired if the Federal Court had been informed of the incident. CSIS responded that it had not done so prior to the Court granting these new powers. [47] When asked who was responsible for not informing the Court of this incident, CSIS responded:

---

[43] In general, the is responsible for ensuring that the intended execution of warrant powers is supported by the applicable warrant. Should questions arise concerning the interpretation of warrants or the legality of conducting specific warranted or non-warranted operations, the is to seek guidance from HQ Legal Services. For questions related to process and procedures, the is to seek guidance from HQ/

[44] Refer to email, "Follow-on Request to – | Briefing – Review ,"

[45] In particular, the " will be communicating directly with the to ensure that she is cc`d on all ". Refer to CSIS Email, "RE: – Actions Taken,"

[46] CSIS Email, " – Non-compliance with warrant ,"

[47] CSIS initially responded to this question with the following: "With regard to the question of whether the Federal Court informed of the non-compliance, has confirmed that the Federal Court was not informed of this specific incident. In 2015 03, the court was informed of the need to expand the powers contained in the s.16 warrants, which includes ." Refer to Email, " Visit – Non Compliance Questions – Review ," July 21, 2016.

ATIP version FEB 25 2019 dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

> There was no decision not to inform the Court as it has not been the practice of the Service to inform the Federal Court of situations where it may have acted without legal authority or contravened the law.[48]

CSIS's warrant activities must conform to what was initially prescribed by the Federal Court, and in cases where it failed to do so, it is SIRC's opinion that the Court would benefit from this knowledge so as to prescribe whatever the Court deems appropriate in that circumstance. It is therefore a positive development that the Department of Justice and CSIS are jointly working on a series of measures aimed at reinforcing the capacities of both organizations to discharge their obligation to the Federal Court. In particular, the measures being proposed include the following:

1.
2.

3.

4.
5.

SIRC believes these additional measures will further enhance accountability. Alongside these, **SIRC makes the following recommendations directed at change internal to CSIS that flow from the overall observations of its review:**

- **that all employees with warranted related responsibilities receive standardized and comprehensive training on an ongoing basis, and that those responsible for providing legal advice have up to date knowledge about technical operations;**
- **that have clearly defined roles and responsibilities which are coordinated and standardized across the regions; and,**
- **that CSIS create a s.21 policy centre devoted to the execution of warrants.**

Should be retained within the regions following the creation of the s.21 policy centre, CSIS should also ensure that there are national standards for the hiring, training and job expectations of this cadre of employee.

[48] The CSIS quote concluded that: "As you are aware, the matter was reported to the Minister of Public Safety via the Director's Annual Report to the Minister, which is subsequently certified by SIRC, as per the accountability structure set forth in the *CSIS Act*." Refer to Memo, "SIRC Study 2016-02, CSIS's Warranted Collection of Information: Operations," August 22, 2016.

[49] Department of Justice document, June 8, 2016.

ATIP version dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

6 CONCLUSION

This review focused on CSIS's compliance with warrants in three specific contexts, focusing first on operations and then more generally with respect to the processing of intercept material. Finally, the review examined an incidence of non-compliance that occurred in . Several interrelated themes have been underscored here, including the importance of CSIS consulting with NSLAG when there is the "slimmest doubt"[50] to ensure that warrants are executed on the basis of considered legal advice. This complements earlier SIRC reviews that also emphasize the need for CSIS to seek legal advice in certain situations and to take steps to make that advice available to other areas of CSIS. SIRC acknowledges the work done toward this end, including making legal opinions available on CSIS's internal website.

At the same time, SIRC recognizes that the execution of warrant powers is a routine part of CSIS operations; thus not every execution requires formal or informal legal advice. To that end, all the cases presented here underscore the necessity of providing employees with warrant related responsibilities the benefit of training on warrants on an ongoing basis.

The timing of this review is fortunate in that CSIS is instituting improvements to its processes surrounding the execution of warrants, in part through . SIRC also understands that there are efforts underway to sensitize CSIS employees on warrant compliance issues.[51] SIRC is hopeful that its findings and recommendations will contribute to these efforts.

[50] CSIS response to SIRC memo, 25 August 2016
[51] Refer to SIRC meeting with and NSLAG, August 16, 2016

ATIP version
dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FINDINGS

SIRC found that the regions, in concert with HQ, did make efforts to

SIRC found that it was problematic that information and the justification were not included in the RIS.

SIRC found that not including information in the RIS, and information justifying created a risk of non-compliance with the warrant.

SIRC found that the new SOPs with respect to the RIS reflect the requirement to

SIRC found that a gap has slowly developed between CSIS's use of technology and the management of critical compliance functions.

SIRC found that warrant training for employees is not consistent across job functions.

SIRC found that CSIS has not created consistent standards for the hiring, training and job functions expected of

ATIP version
dated: FEB 2 5 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RECOMMENDATIONS

SIRC makes the following recommendations:

- **that all employees with warranted related responsibilities receive standardized and comprehensive training on an ongoing basis, and that those responsible for providing legal advice have up to date knowledge about technical operations;**
- **that have clearly defined roles and responsibilities which are coordinated and standardized across the regions; and,**
- **that CSIS create a s.21 policy centre devoted to the execution of warrants.**

Should be retained within the regions following the creation of the s.21 policy centre, CSIS should also ensure that there are national standards for the hiring, training and job expectations of this cadre of employee.

ATIP version
FEB 2 5 2019
dated: